



universität
wien

MASTER THESIS

Titel der Master Thesis / Title of the Master's Thesis

„Identifizierungspflicht und Klarnamenzwang in Internetforen“

„Grundrechtliche Probleme einer ‚digitalen Ausweispflicht‘ am Beispiel des
Entwurfs des Bundesgesetzes über Sorgfalt und Verantwortung im Netz“

verfasst von / submitted by

Mag. Markus Sagmeister

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of
Master of Laws (LL.M.)

Wien, 2022 / Vienna 2022

Studienkennzahl lt. Studienblatt /
Postgraduate programme code as it appears on
the student record sheet:

UA 992 942

Universitätslehrgang lt. Studienblatt /
Postgraduate programme as it appears on
the student record sheet:

Informations- und Medienrecht

Betreut von / Supervisor:

HR Hon.-Prof. Dr. Hans Peter Lehofer

Inhaltsverzeichnis

Abkürzungsverzeichnis.....	VII
1. Einleitung - Die Suche nach rechtlichen Mitteln gegen „Hass im Netz“	1
2. Ziel der Arbeit und Methodik.....	7
3. Analyse des Gesetzestextes des Ministerialentwurfs des SVN-G.....	9
3.1 Welche Foren sind betroffen?	9
3.2 Die Übermittlungspflichten des SVN-G	11
3.2.1 Übermittlung an Dritte	11
3.2.2 Übermittlung an Behörden, Staatsanwaltschaften und Gerichte	12
3.3 Die Registrierungs- und Identifizierungspflichten des SVN-G	13
3.3.1 Nutzerdaten stellen personenbezogene Daten dar	14
3.3.2 Pflicht zur Überprüfung der Identität der Nutzer.....	14
3.3.3 Pflicht zur periodischen Überprüfung der Nutzerdaten	17
3.3.4 Pflicht zur Überprüfung der regelmäßigen Aktivität der Nutzer	17
3.4 Pflicht zur Speicherung und Übermittlung von Postinginhalten	18
3.4.1 Postings stellen personenbezogene Daten dar	19
3.4.2 Ist die Löschung von Postings dennoch erlaubt?	21
3.4.3 Anwendung des Medienprivilegs auf Postings.....	24
3.5 Löschpflichten betreffend das Registrierungsprofil.....	26
3.6 Verbot der Verknüpfung von Nutzerdaten.....	28
3.7 Ergebnis der Analyse des Gesetzestextes des SVN-G.....	29
3.7.1 Einschränkung auf bestimmte Kategorien von Internetforen	29
3.7.2 Konflikt mit dem Herkunftslandprinzip.....	31
4. SVN-G bewirkt anlasslose Vorratsdatenspeicherung	33
4.1 Parallelen zur Vorratsdatenspeicherung von Telekommunikationsdaten.....	36
4.1.1 Eingriffe in elektronische Kommunikation	36
4.1.2 Ähnlichkeit der betroffenen Datenkategorien.....	38
4.2 Unterschiede zur Vorratsdatenspeicherung von Telekommunikationsdaten.....	39

5.	Grundrechtsprüfung.....	41
5.1	Prüfungsmaßstab der Grundrechtsprüfung	42
5.2	VfGH-Rechtsprechung betreffend anlasslose Vorratsdatenspeicherung	43
5.3	Liegen Eingriffe in die genannten Grundrechte vor?.....	43
5.4	Exkurs: Verletzung des Wesensgehalts der betroffenen Grundrechte?	45
5.5	Verhältnismäßigkeitsprüfung	48
5.5.1	Liegen die Ziele des SVN-G im öffentlichen Interesse?	49
5.5.2	Eignung der Maßnahmen zur Erreichung der Ziele.....	50
5.5.3	Erforderlichkeit der Eingriffsmaßnahmen des SVN-G.....	51
5.6	Adäquanz - Verhältnismäßigkeit im engeren Sinn	55
5.6.1	Maßnahmen sind nur zur Verfolgung schwerer Straftaten zulässig	56
5.6.2	Betroffener Personenkreis zu weit gefasst	58
5.6.3	Gefahr des Datenmissbrauchs und des unbefugten Zugriffs	60
5.6.4	Materiell- und verfahrensrechtliche Regeln für den Zugang zu den Daten....	62
5.6.5	Vorprüfung und Kontrolle durch Gericht oder unabhängige Behörde	64
5.6.6	Gefahr des „Overblocking“	66
5.6.7	Technische und organisatorische Maßnahmen zum Schutz der Daten.....	67
5.6.8	Zeitstempel sind nicht verhältnismäßig	69
5.6.9	Löschpflichten und zeitlich begrenzte Speicherdauer	69
5.6.10	Speicherung der Nutzerdaten im Unionsgebiet	70
5.6.11	Identifizierungspflicht des SVN-G bewirkt „chilling effects“	71
5.7	Ergebnis der Grundrechtsprüfung.....	73
6.	Conclusio - Eignung von Identifizierungs- und Klarnamenpflichten zur Bekämpfung von „Hass im Netz“	79
7.	Literaturverzeichnis.....	81
8.	Rechtsquellenverzeichnis.....	89
9.	Judikaturverzeichnis	93
10.	Anhang	95
10.1	Anhang 1: Ministerialentwurf des SVN-G	95
10.2	Anhang 2: Erläuterungen zum Ministerialentwurf des SVN-G	103
11.	Abstract (Deutsch)	111
12.	Abstract (English)	113

Abkürzungsverzeichnis

ABGB	Allgemeines Bürgerliches Gesetzbuch
ABl	Amtsblatt der Europäischen Union
Abs	Absatz
Anm. d. Verf.	Anmerkung des Verfassers
Art	Artikel
BGBI	Bundesgesetzblatt
bzw	beziehungsweise
DSB	Datenschutzbehörde
DSG	Datenschutzgesetz
DSGVO	Datenschutz-Grundverordnung
ECG	E-Commerce-Gesetz
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
EU	Europäische Union
EuGH	Europäischer Gerichtshof
f	folgende
ff	fortfolgende
FinStrG	Finanzstrafgesetz
FPÖ	Freiheitliche Partei Österreichs
GA	Generalanwalt am Europäischen Gerichtshof bzw. Schlussanträge des Generalanwalts
GP	Gesetzgebungsperiode
GRC	Charta der Grundrechte der Europäischen Union
Grüne	Die Grünen – Die Grüne Alternative
GSMA	GSM Association
HiNBG	Hass-im-Netz-Bekämpfungs-Gesetz
Hrsg	Herausgeber
idF	in der Fassung
iS	im Sinne
iSd	im Sinne des
iVm	in Verbindung mit

KoPl-G	Kommunikationsplattformen-Gesetz
lit	litera
ME	Ministerialentwurf
MR	Medien und Recht (Zeitschrift)
NetzDG	Netzwerkdurchsetzungsgesetz
Nr	Nummer
OGH	Oberster Gerichtshof
ÖJZ	Österreichische Juristen-Zeitung
ÖVP	Österreichische Volkspartei
PresseFG 2004	Presseförderungsgesetz 2004
PrR-G	Privatradiogesetz
PStSG	Polizeiliches Staatsschutzgesetz
RIS	Rechtsinformationssystem des Bundes
RL	Richtlinie
Rz	Randziffer
SPG	Sicherheitspolizeigesetz
StGB	Strafgesetzbuch
StGG	Staatsgrundgesetz
StPO	Strafprozessordnung
SVN-G	Bundesgesetz über Sorgfalt und Verantwortung im Netz
TKG / TKG 2003	Telekommunikationsgesetz 2003
u.a. / ua	und andere
ÜKVO	Überwachungskostenverordnung
VfGH	Verfassungsgerichtshof
VfSlg	Ausgewählte Entscheidungen des Verfassungsgerichtshofes
Vgl	vergleiche
Z	Ziffer
ZÖR	Zeitschrift für öffentliches Recht

1. Einleitung - Die Suche nach rechtlichen Mitteln gegen „Hass im Netz“

Das Internet ermöglicht es durch ein stetig wachsendes Angebot an vielfältigsten Diskussionsforen und sozialen Netzwerken, sich jederzeit weltweit mit anderen Menschen zu allen erdenklichen Themen ungehindert auszutauschen. Auf den digitalen Plattformen dieser vernetzten Welt hat es sich dabei weitgehend etabliert, unter Verwendung sogenannter Nicknames zu kommunizieren, um den Nutzern auf diese Weise zu gewähren, ihre Identität und ihren bürgerlichen Namen schützen zu können. Die so gewonnene Anonymität eröffnet den Menschen die prinzipielle Chance, ihre Meinung im Netz unbeeinflusst äußern zu können, was vor allem in Staaten von besonderer Bedeutung ist, in denen den Bürgern nicht derselbe Grad an Meinungsfreiheit zugestanden wird, den man in demokratischen Gesellschaften gewohnt ist.

Wie auch im „analogen Leben“ ist es auch bei Diskussionen im Internet naturgemäß nicht vermeidbar, dass es gelegentlich zu Untergriffen durch manche Nutzer kommt, bis hin zu beleidigenden Äußerungen, die Verletzungen von Persönlichkeitsrechten bewirken oder sogar Straftatbestände erfüllen, die bis zu schwerwiegenden Delikten wie Verhetzung oder nationalsozialistischer Wiederbetätigung reichen können. Es bestehen jedoch Anzeichen, wonach die Hemmschwelle, sich zu solchen rechtswidrigen Äußerungen hinreißen zu lassen, bei manchen Menschen im Internet deutlich niedriger liegt,¹ was sich auch in steigenden Fallzahlen solcher Vorfälle niederschlägt. Dieses Phänomen, für das sich Schlagworte wie „Hass im Netz“, „Hassrede“ oder „Hate Speech“ eingebürgert haben, hat sich im Laufe der Zeit zu einem zunehmend größeren Problem mit entsprechender medialer Präsenz entwickelt.² Auch die Politik hat das Thema „Hass im Netz“ in den vergangenen Jahren immer öfter aufgegriffen, wohl nicht zuletzt deshalb, weil auch regelmäßig bekannte Persönlichkeiten des öffentlichen Lebens oder Politiker selbst betroffen sind. In Österreich

¹ Burger, Sch(m)utz im Netz. Warum wir digitale Masken brauchen (2021) 29 ff.

² Kurier, Website 23.09.2020, Hass im Netz: ZARA verzeichnete starken Anstieg bei Meldungen <www.kurier.at/politik/inland/hass-im-netz-zara-verzeichnete-starken-anstieg-bei-meldungen/401041340> (abgefragt am 14.01.2022);

Der Standard, Website 25.11.2016, Verhetzung: Fast wöchentlich Prozesse gegen Hassposter <www.derstandard.at/story/2000048178327/verhetzung-fast-woechentlich-prozesse-gegen-hassposter> (abgefragt am 14.01.2022).

vielbeachtet waren beispielsweise die Fälle um Eva Glawischnig-Piesczek,³ Sigrid Maurer⁴ und Armin Wolf bzw Heinz-Christian Strache,⁵ die auch zu einer verstärkten juristischen Auseinandersetzung mit dem Thema „Hass im Netz“ geführt haben.

Im Zusammenhang damit ist auch die auf den meisten Diskussionsplattformen übliche Anonymität der Nutzer zunehmend in die Kritik politischer Parteien geraten. So sehen manche darin ein förderliches Element für „Hass im Netz“, wenn nicht sogar die Ursache selbst, da ihrer Ansicht nach die Anonymität die an sich schon niedrige Hemmschwelle im Netz noch weiter senke.

Als mögliche Maßnahme, um diesem Problem entgegenzuwirken, wird von Kritikern der Anonymität immer wieder die Idee einer sogenannten Klarnamenpflicht ins Spiel gebracht. Darunter ist eine gesetzliche Regelung zu verstehen, die das Posten von Kommentaren nur noch unter sichtbarer Anführung des bürgerlichen Namens des jeweiligen Nutzers erlauben soll. Eine Verwendung von Nicknames wäre also nicht mehr zulässig, und die Anonymität in den betroffenen Foren damit beseitigt. Dies soll die Verfasser von Hasspostings eindeutig identifizierbar machen, da bei Foren ohne verpflichtende Identifizierung in manchen Fällen keine korrekten Identitätsdaten der Nutzer vorliegen. Demnach sei das zu lösende Grundproblem, dass die Ausforschung der Täter zu oft scheitere.⁶

Verfechter der Anonymität hingegen sehen in dieser ein unverzichtbares Mittel zur Sicherung und Förderung der freien Meinungsäußerung und Meinungsbildung im Netz und warnen vor der Gefahr einer Instrumentalisierung einer solchen Klarnamenpflicht, etwa um

-
- ³ Der Standard, Website 12.11.2020, Oberster Gerichtshof: Facebook muss Hassposting gegen Glawischnig weltweit löschen <www.derstandard.at/story/2000121648569/oberster-gerichtshof-verfuegt-facebook-muss-hassposting-gegen-glawischnig-weltweit-loeschen> (abgefragt am 14.01.2022);
OGH 15.09.2020, 6 Ob 195/19y;
EuGH 03.10.2019, C-18/18 (Glawischnig-Piesczek);
Zankl, Host-Provider: Löschung rechtswidriger wort- und sinngleicher Postings, *ecolex* 2021/10, 24 (24);
Lehofer, Hass im Netz und gedruckt: europäische Gerichte, österreichische Fälle, *ÖJZ* 2019/112, 893.
- ⁴ *Löwenstein*, Der Hass, das Netz und der Tod, Website Frankfurter Allgemeine Zeitung 04.07.2021 <www.faz.net/aktuell/politik/der-hass-das-netz-und-der-tod-17418839> (abgefragt am 14.01.2022).
- ⁵ *Silber*, Facebook muss Straches "Lügen"-Posting zu Armin Wolf in Österreich löschen, Website Kurier 04.05.2020 <www.kurier.at/kultur/medien/facebook-muss-straches-luegen-posting-zu-armin-wolf-in-oesterreich-loeschen/400831475> (abgefragt am 14.01.2022);
OGH 30.03.2020, 4 Ob 36/20b.
- ⁶ *Wittmann/Zöchbauer*, Zum Entwurf eines Bundesgesetzes über Sorgfalt und Verantwortung im Netz. Ein kritischer Überblick, *MR* 2019, 103 (103).

die Äußerung von Kritik an bestimmten politischen Entwicklungen zu erschweren, oder kritischen Diskussionsplattformen gezielt zu schaden. Gegner von Klarnamenpflichten vertreten zudem teils die Ansicht, dass die Ausforschung der Täter in den meisten Fällen auch mit den bereits zur Verfügung stehenden Mitteln der Rechtsordnung in ausreichendem Maß möglich sei. Die Problematik und das häufige Auftreten von Hasspostings seien eher darin begründet, dass gewisse Rechtslücken bzw -mängel bewirken, dass einerseits die prozessuale Durchsetzung oft zu aufwendig oder mit zu hohem Kostenrisiko für die Betroffenen verbunden und zudem bestimmte Erscheinungsformen von „Hass im Netz“ zwar gesellschaftlich missbilligt, jedoch weder strafbar noch zivilrechtlich verfolgbar seien.⁷ Dies könne vor allem in den Tätern den Eindruck erwecken, dass Hasskommentare aufgrund der in manchen Fällen ausbleibenden Konsequenzen mitunter sogar von der Meinungsäußerungsfreiheit gedeckt seien.

Die Diskussionen um Klarnamen- und Identifizierungspflichten beschränken sich aber nicht nur auf Österreich, sondern diese werden international geführt.⁸ So war etwa in Südkorea bereits von 2007 bis 2012 eine Klarnamenpflicht in Kraft, die jedoch in erster Linie wegen ihrer Ineffizienz und spektakulären Fällen von Diebstahl der gespeicherten Identitätsdaten der Bürger durch Hackerangriffe für Schlagzeilen sorgte und letztlich vom südkoreanischen Verfassungsgericht wegen Unvereinbarkeit mit dem Recht auf Meinungsfreiheit aufgehoben wurde.⁹ Der deutsche Gesetzgeber hat zwischenzeitig versucht, mit einem anderen Ansatz, nämlich dem sogenannten „Netzwerkdurchsetzungsgesetz“ (NetzDG) auf das Problem „Hass im Netz“ zu reagieren.¹⁰ Das NetzDG sieht im Gegensatz zu einer Klarnamenpflicht keinen Identifizierungszwang vor, sondern nimmt stattdessen die Forenbetreiber in die Pflicht, rechtswidrige Postings möglichst rasch zu entfernen.

⁷ *Windhager/Forgó*, Hasspostings. Bedarf es einer gesetzlichen Verschärfung? AnwBl 2017/98, 592 (592).

⁸ *Steinke*, Wer Klarnamen im Netz fordert, hat Bürgerrechte nicht verstanden, Website Süddeutsche Zeitung 12.06.2019 <www.sueddeutsche.de/digital/social-media-klarnamenpflicht-union-internet-1.4482238> (abgefragt am 14.01.2022).

⁹ *Brodnig*, Der unsichtbare Mensch. Wie die Anonymität im Internet unsere Gesellschaft verändert (2013) 141 ff;
Futurezone, Website 23.08.2012, Klarnamenzwang in Südkorea ist verfassungswidrig <www.futurezone.at/netzpolitik/klarnamenzwang-in-suedkorea-ist-verfassungswidrig/24.584.187> (abgefragt am 14.01.2022).

¹⁰ Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG) vom 1. September 2017, dBGBI I S 3352 idF I S 1436; Deutsches Bundesministerium der Justiz und für Verbraucherschutz, Website <www.gesetze-im-internet.de/netzdg/index.html> (abgefragt am 14.01.2022).

Während in Frankreich zuletzt ein ähnlich gelagertes Gesetz gegen „Hass im Netz“, das sogenannte „Loi Avia“, am französischen Verfassungsgericht gescheitert ist,¹¹ scheint das deutsche NetzDG vorerst Bestand zu haben. Trotz dieses Lösungsversuchs sind aber auch in Deutschland die Rufe nach einem Klarnamen- bzw Identifizierungszwang bis heute nicht verstummt,¹² ebenso wenig wie auf europäischer Ebene.¹³

In Österreich hat die im Dezember 2017 neu angetretene, von ÖVP und FPÖ gebildete Bundesregierung mit Plänen aufhören lassen, sich des Themas „Hass im Netz“ durch die Einführung eines „digitalen Vermummungsverbots“ annehmen zu wollen.¹⁴ Im April 2019 haben Regierungsvertreter schließlich medienwirksam den Ministerialentwurf für ein Gesetz mit dem Titel „Bundesgesetz über Sorgfalt und Verantwortung im Netz“ (SVN-G) vorgestellt.¹⁵

In diesem Gesetzesentwurf ist vorgesehen, dass einem Nutzer das Posten in bestimmten Internetforen nur noch nach verpflichtender Registrierung mittels Name und Adresse und erfolgreicher Identitätsüberprüfung durch die Forenbetreiber gestattet sein soll. Dieser von der Regierung als „digitale Ausweispflicht“ angepriesene Identifizierungszwang stellt insofern eine Art „indirekte Klarnamenpflicht“ dar, als dabei die bürgerlichen Namen zwar nicht im Forum sichtbar angeführt werden müssen (die Verwendung von Nicknames bliebe also erlaubt), aber dennoch die Personalien sämtlicher Nutzer von den Forenbetreibern zu erheben und intern zu speichern sind, um später, beim Auftreten rechtswidriger Postings, zur Identifizierung des betreffenden Nutzers darauf zurückgreifen zu können.

¹¹ *Wienfort*, Blocking Overblocking. Frankreichs Verfassungsrat kippt das Gesetz gegen Hasskriminalität im Netz, Website Verfassungsblog.de 20.06.2020 <www.verfassungsblog.de/blocking-overblocking> (abgefragt am 14.01.2022).

¹² *Neuerer*, Schäuble fordert Klarnamenpflicht im Netz, Website Handelsblatt 13.01.2020 <www.handelsblatt.com/politik/deutschland/hass-im-internet-schaeuble-fordert-klarnamenpflicht-im-netz/25424450.html?ticket=ST-308700-cAmVkaJJcOapHSJd9SmD-ap6> (abgefragt am 14.01.2022).

¹³ *Süddeutsche Zeitung*, Website 17.05.2019, Union für Klarnamenpflicht im Internet <www.sueddeutsche.de/politik/facebook-weber-schaeuble-klarnamen-1.4451908> (abgefragt am 14.01.2022).

¹⁴ *ORF.at*, Website 13.11.2018, Regierung will „Vermummungsverbot“ <www.orf.at/stories/3100546> (abgefragt am 14.01.2022).

¹⁵ *ME Bundesgesetz über Sorgfalt und Verantwortung im Netz (SVN-G)*, Gesetzestext, 134/ME XXVI. GP <www.parlament.gv.at/PAKT/VHG/XXVI/ME/ME_00134/fname_747395.pdf> (abgefragt am 14.01.2022).

Das SVN-G, das im Übrigen nicht nur unter Datenschützern und Grundrechtsaktivisten überwiegend auf Ablehnung stieß,¹⁶ ist deshalb bemerkenswert, weil in Österreich damit zum ersten Mal der Entwurf eines vollständigen Gesetzes vorgelegt worden ist, das einen Identifizierungszwang für sämtliche Bürger vorsieht, die bestimmte Internetforen nutzen möchten.

Auch wenn das SVN-G bis heute nicht in Kraft getreten ist, nicht zuletzt aufgrund des jähen Endes der ÖVP-FPÖ-Regierungskoalition nach der sogenannte Ibiza-Affäre im Mai 2019 nur wenige Wochen nach der Vorstellung des Ministerialentwurfs, und der Entwurf auch von den Nachfolgeregierungen bis dato nicht mehr weiterverfolgt worden ist, blieben die Forderungen nach Schritten zur Eindämmung von „Hass im Netz“ weiter aufrecht.

Die ab Jänner 2020 amtierende Koalitionsregierung aus ÖVP und Grünen hat wiederum zwischenzeitig mit einem neuen, grundlegend anders gestalteten Maßnahmenpaket gegen „Hass im Netz“ reagiert, welches zwar ebenfalls nicht kritiklos geblieben ist, aber auf den ersten Blick dennoch weniger einschneidend wirkt als das SVN-G, da es auf einen Identifizierungs- oder Klarnamenzwang verzichtet.

Dieses am 01.01.2021 in Kraft getretene Gesetzespaket beinhaltet zum einen das neue Kommunikationsplattformen-Gesetz (KoPl-G),¹⁷ dessen Hauptaugenmerk, ähnlich dem deutschen NetzDG, vor allem auf Löschpflichten für Betreiber von Kommunikationsplattformen liegt. Diese werden dadurch verpflichtet, rechtswidrige Postings binnen 24 Stunden bzw sieben Tagen zu entfernen. Zusätzlich führt das Gesetzespaket das Hass-im-Netz-Bekämpfungs-Gesetz (HiNBG)¹⁸ neu ein, das eine Reihe von kleineren Gesetzesanpassungen enthält, die in erster Linie die Rechtsverfolgung bei Verletzungen von Persönlichkeitsrechten erleichtern sollen. Beispielsweise wurde damit die Möglichkeit eröffnet, bei den Bezirksgerichten die gerichtliche Löschung von Hasspostings ohne vorangehende Verhandlung zu erwirken, durch Einbringung einer Klage samt Antrag auf Erlassung eines

¹⁶ Der Standard, Website 10.05.2019, Digitale Ausweispflicht: Gesetz stößt auf Skepsis bei Experten <www.derstandard.at/story/2000102900226/digitaler-ausweiszwang-gesetz-stoesst-auf-skepsis-bei-experten> (abgefragt am 14.01.2022);

Al-Youssef, Regierung will Anonymität im Netz abschaffen – mit hohen Strafen, Website Der Standard 10.04.2019 <www.derstandard.at/story/2000101143621/regierung-will-anonymitaet-im-netz-abschaffen-mit-hohen-straften> (abgefragt am 14.01.2022).

¹⁷ Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen (Kommunikationsplattformen-Gesetz – KoPl-G), BGBl I 151/2020.

¹⁸ Bundesgesetz, mit dem Maßnahmen zur Bekämpfung von Hass im Netz getroffen werden (Hass-im-Netz-Bekämpfungs-Gesetz – HiNBG), BGBl I 148/2020.

Unterlassungsauftrags im Mahnverfahren. Außerdem wurde unter anderem auch ein Antrag auf Herausgabe von Nutzerdaten gemäß § 18 Abs 4 E-Commerce-Gesetz (ECG)¹⁹ im außerstreitigen Verfahren geschaffen, neben einigen weiteren Neuerungen und Änderungen, die Aufwand und Prozessrisiko für von Hasspostings Betroffene verringern sollen.²⁰ Bei diesem Gesetzespaket handelt es sich aber voraussichtlich nur um einen Zwischenschritt. Denn auf EU-Ebene plant man mit dem sogenannten „Digital Services Act“ alsbald einen für alle Mitgliedstaaten einheitlichen Rechtsrahmen zu schaffen, der auch dem Problem „Hass im Netz“ entgegensteuern soll.²¹ Dabei ist aktuell noch nicht absehbar, inwiefern das derzeitige österreichische Gesetzespaket letztendlich mit dieser europarechtlichen Regelung vereinbar sein wird.

Auch wenn die Identifizierungspflicht des SVN-G in Österreich nun wohl nicht mehr umgesetzt wird, und auch die aktuellen EU-Vorhaben wie der „Digital Services Act“ derzeit keine derartigen Bestrebungen vorsehen, so bedeutet dies aber keineswegs, dass die Einführung von Identifizierungs- oder Klarnamenpflichten zukünftig ausgeschlossen ist. So hat sich etwa nach mehreren Terroranschlägen in der jüngeren Vergangenheit gezeigt, dass die politische Stimmungslage in Europa sehr schnell hin zu einem Ruf nach mehr Überwachung im Internet kippen kann.²²

¹⁹ Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz – ECG), BGBl I 152/2001 idF I 148/2020.

²⁰ Zankl/Knaipp, Neues IT-Recht, ecolex 2021/73, 106 (106).

²¹ Grimm, Neues EU-Gesetz könnte Hass im Netz mindern, Website Die Presse 15.01.2021 <www.diepresse.com/5922905/neues-eu-gesetz-konnte-hass-im-netz-mindern> (abgefragt am 14.01.2022);

Europäische Union, Website, Gesetz über digitale Dienste: mehr Sicherheit und Verantwortung im Online-Umfeld <ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_de> (abgefragt am 14.01.2022).

²² Kühl, Mehr Überwachung ist verständlich – und trotzdem falsch, Website Zeit Online 17.11.2015 <www.zeit.de/digital/datenschutz/2015-11/vorratsdatenspeicherung-ueberwachung-paris-anschlag-terrorismus> (abgefragt am 14.01.2022).

2. Ziel der Arbeit und Methodik

Das Ziel dieser Arbeit ist es daher, anhand einer eingehenden Analyse der Maßnahmen des Entwurfs des SVN-G, die Auswirkungen aufzuzeigen, die eine Identifizierungspflicht oder die vergleichbare Variante eines direkten Klarnamenzwangs in Österreich vor allem im Hinblick auf die verfassungsgesetzlich gewährleisteten Rechte der Bürger, welche die betroffenen Diskussionsplattformen nutzen, zur Folge hätte. Am Beispiel des SVN-G lässt sich dies deshalb ideal veranschaulichen, weil es sich dabei nicht bloß um ein fiktives Konzept einer Identifizierungspflicht handelt, sondern um den realen Entwurf eines vollumfänglichen Gesetzes, das eine solche verpflichtende Identifizierung sämtlicher Nutzer bestimmter Diskussionsforen anordnet.

Dazu werden zunächst durch eine Analyse des Gesetzestextes des SVN-G jene Bestimmungen herausgearbeitet, die sich auf die Rechte der Nutzer der betroffenen Diskussionsplattformen auswirken. Anschließend werden die einzelnen im SVN-G konkret zur Zielerreichung vorgesehenen Maßnahmen identifiziert und danach auf ihre Vereinbarkeit mit den Grundrechten der Nutzer untersucht. Als Prüfungsmaßstab wird dabei die Rechtsprechung der österreichischen und europäischen Höchstgerichte zu vergleichbaren Fällen herangezogen. Bei dieser Grundrechtsprüfung sollen die Maßnahmen des SVN-G unter anderem auf ihre Erforderlichkeit und Verhältnismäßigkeit geprüft und dabei auch den zum Zeitpunkt der Veröffentlichung des Ministerialentwurfs in der österreichischen Rechtsordnung bereits vorhandenen Möglichkeiten zur Verfolgung von aus Hasspostings resultierenden Straftaten und Rechtsansprüchen gegenübergestellt werden.

Im Ergebnis soll so festgestellt werden, ob eine Identifizierungspflicht betreffend sämtliche Nutzer bestimmter Kategorien von Diskussionsplattformen, wie sie der Ministerialentwurf des SVN-G vorsieht, geeignet ist, um den durch „Hass im Netz“ verursachten grundlegenden Problemen effektiv und in verhältnismäßiger Weise entgegenzuwirken, ohne dabei die Grundrechte der Bürger zu verletzen.

3. Analyse des Gesetzestextes des Ministerialentwurfs des SVN-G

Im ersten Schritt gilt es die Bestimmungen des Normtextes des Entwurfs des SVN-G herauszuarbeiten, die sich unmittelbarer oder in indirekter Weise auf die Rechtspositionen der Nutzer der betroffenen Foren auswirken und der Erreichung der vorrangigen Ziele des SVN-G dienen. Regelungen, die hingegen vorwiegend die Rechte der Forenbetreiber betreffen und für die Nutzer weniger relevant sind, werden gegebenenfalls am Rande erläutert.

Das primäre Ziel des SVN-G ist es, die Strafverfolgung und Durchsetzung von Rechtsansprüchen gegen die Verfasser von rechtswidrigen Postings in Internetforen zu erleichtern, indem die Betreiber von betroffenen Foren dazu verpflichtet werden, den Namen und die Adresse eines jeden Nutzers vorab zu speichern und bei Bedarf offenzulegen. Um dies zu ermöglichen, sieht das Konzept des SVN-G vor, dass jede Person, die in einem Diskussionsforum Kommentare posten möchte, sich zuvor gegenüber dem Betreiber des Forums identifizieren muss, indem sie diesem in einem verpflichtenden Registrierungsvorgang ihren Namen und ihre Adresse bekanntgibt und die Richtigkeit dieser Daten zusätzlich belegt, beispielsweise durch Vorlage von Dokumenten. Der Betreiber ist verpflichtet, diese Registrierung und Identifizierung sämtlicher Nutzer durchzuführen, andernfalls darf er diesen das Veröffentlichen von Kommentaren im Forum nicht gestatten. Die Normadressaten des SVN-G sind somit die Betreiber der betroffenen Foren, die sogenannten Diensteanbieter, und nicht etwa die Nutzer. Den Diensteanbietern obliegt es, für die Umsetzung der durch das SVN-G auferlegten Pflichten zu sorgen.

3.1 Welche Foren sind betroffen?

Das SVN-G findet jedoch nicht auf alle erdenklichen, sondern nur auf bestimmte Diskussionsforen, die konkrete Kriterien erfüllen, Anwendung.

Gemäß § 3 Abs 1 SVN-G richtet sich der Entwurf an sogenannte „Diensteanbieter eines Online-Informationsangebotes“²³ und zwar an jene, die „als Bestandteil des Dienstes selbst ein Forum einrichten und betreiben, das auf Nutzer in Österreich ausgerichtet ist, oder [...]

²³ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 1.

im Rahmen ihres Dienstes die Einrichtung eines wie in Z 1 beschriebenen Forums durch die Nutzer ihres Dienstes ermöglichen“²⁴.

Den Begriff „Forum“ definiert das SVN-G in § 2 Z 3 als „die online-Funktion zum Austausch von Mitteilungen oder Darbietungen mit gedanklichem Inhalt (Posting) von Nutzern mit einem größeren Personenkreis anderer Nutzer“²⁵.

Die Verpflichtungen des SVN-G treffen jedoch nur solche Diensteanbieter, auf die zumindest eine der vier in § 3 Abs 2 SVN-G taxativ aufgezählten Bedingungen zutrifft. Demnach ist das SVN-G einerseits nur auf solche Diensteanbieter anzuwenden, „deren Dienst im Inland mehr als 100.000 registrierte Nutzer hat“²⁶, gemäß § 3 Abs 2 Z 1 SVN-G oder „deren im vorangegangenen Jahr in Österreich erzielter Umsatz 500.000 Euro übersteigt“²⁷, gemäß § 3 Abs 2 Z 2 SVN-G. Des Weiteren fallen in den Anwendungsbereich des SVN-G „Medieninhaber, die im vorangegangenen oder aktuellen Kalenderjahr Fördermittel nach dem Presseförderungsgesetz, BGBl. I Nr. 136/2003 [PresseFG 2004²⁸ - *Anm. d. Verf.*] von mehr als 50.000 Euro erhalten haben oder erhalten“²⁹, gemäß § 3 Abs 2 Z 3 SVN-G sowie „für mit einem nach Z 3 erfassten Medieninhaber im Sinne von § 9 Abs. 4 PrR-G, BGBl I Nr. 20/2001 [Privatradiogesetz³⁰ - *Anm. d. Verf.*] verbundene Diensteanbieter, soweit sie mit ihrem Online-Informationsangebot unter der gleichen oder einer ähnlichen Marke auftreten wie der nach Z 3 erfasste Fördermittelempfänger“³¹, gemäß § 3 Abs 2 Z 4 SVN-G.

In den Erläuterungen zum Entwurf findet sich als Erklärung, dass man mit dieser Eingrenzung den Anwendungsbereich auf solche Diensteanbieter einschränken wolle, denen man aufgrund ihrer Größe die Einrichtung der nötigen technischen Maßnahmen zumuten könne.³² Was jedoch die Beweggründe der Verfasser des Entwurfs waren, diese Zumutbar-

²⁴ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 1 Z 1 und 2.

²⁵ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 2 Z 3.

²⁶ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 2 Z 1.

²⁷ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 2 Z 2.

²⁸ Bundesgesetz über die Förderung der Presse (Presseförderungsgesetz 2004 – PresseFG 2004), BGBl I 136/2003 idF I 32/2018.

²⁹ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 2 Z 3.

³⁰ Bundesgesetz, mit dem Bestimmungen für privaten Hörfunk erlassen werden (Privatradiogesetz – PrR-G), BGBl I 20/2001 idF I 86/2015.

³¹ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 2 Z 4.

³² ME Bundesgesetz über Sorgfalt und Verantwortung im Netz (SVN-G), Erläuterungen, 134/ME XXVI. GP, Erläut 3 <www.parlament.gv.at/PAKT/VHG/XXVI/ME/ME_00134/fname_747397.pdf> (abgefragt am 14.01.2022).

keitsschwellen auf konkrete Kennzahlen wie beispielsweise 100.000 registrierte Nutzer oder einen Jahresumsatz von mehr 500.000 Euro festzulegen, erörtern die Erläuterungen nicht.

Keine Anwendung soll das SVN-G hingegen auf Dienste finden, die dem Online-Verkauf oder -Tausch oder der Vermittlung von Waren dienen und die dabei auch ein Forum insbesondere zu Bewertungszwecken anbieten, gemäß § 3 Abs 3 SVN-G.³³

3.2 Die Übermittlungspflichten des SVN-G

Ruft nun ein bestimmtes Posting eines registrierten Forennutzers den Verdacht der Verursachung einer Rechtsverletzung hervor, so sieht das SVN-G zwei Fälle vor, in denen der Diensteanbieter den Namen und die Adresse des Nutzers und zusätzlich das betreffende Posting an den um Übermittlung der Nutzerdaten Ansuchenden herauszugeben hat.

3.2.1 Übermittlung an Dritte

Der erste Fall verpflichtet den Diensteanbieter gemäß § 4 Abs 1 SVN-G zur Übermittlung des Namens und der Adresse des Posters an sogenannte „dritte Personen“³⁴, die ein diesbezügliches „begründetes schriftliches Verlangen“³⁵ vorweisen. Gemäß § 4 Abs 2 SVN-G liegt ein solches begründetes Verlangen im Sinne des Abs 1 „nur dann vor, wenn die dritte Person unter Nachweis ihrer Identität glaubhaft macht, dass die Feststellung der Identität des Posters eine unabdingbare Voraussetzung bildet, um wegen des Inhalts eines Postings gegen dessen Verfasser mittels Privatanklage wegen übler Nachrede (§ 111 Abs. 2 StGB) oder wegen Beleidigung (§ 115 StGB) strafgerichtlich oder wegen Verletzungen an der Ehre (§ 1330 ABGB) zivilgerichtlich vorzugehen.“³⁶

Welche Personen in diesem Zusammenhang mit „dritte Personen“ gemeint sind, lässt sich indirekt aus den in § 4 Abs 2 SVN-G taxativ aufgezählten Tatbeständen schließen. Demnach kommt als „dritte Person“ in Frage, wer Opfer der Privatanklagedelikte der üblen Nachrede (§ 111 Abs 2 StGB) oder der Beleidigung (§ 115 StGB) werden kann, nämlich

³³ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 3.

³⁴ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 4 Abs 1.

³⁵ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 4 Abs 1.

³⁶ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 4 Abs 2.

alle natürlichen Personen.³⁷ Darüber hinaus kommen mögliche Betroffene der zivilrechtlichen Ehrenbeleidigung nach § 1330 ABGB in Betracht, das können sowohl natürliche als auch juristische Personen sein.³⁸

Das Erfordernis eines „begründeten schriftlichen Verlangens“ legt den Schluss nahe, dass vom Diensteanbieter erwartet wird, sich mit der vom Dritten getroffenen Begründung inhaltlich auseinanderzusetzen und zudem wohl auch das Vorliegen eines der drei in § 4 Abs 2 SVN-G angeführten Tatbestände zumindest grob zu prüfen, bevor er die Nutzerdaten an den Dritten herausgibt. Eine Ablehnung eines solchen Verlangens auf Übermittlung von Nutzerdaten durch den Diensteanbieter scheint im Fall des Fehlens dieser formellen Voraussetzungen denkbar, beispielsweise dann, wenn aus Sicht des Diensteanbieters die Glaubhaftmachung des Dritten scheitert, dass die Feststellung der Identität des Posters notwendig ist, um den mutmaßlichen Verstoß gerichtlich zu verfolgen.

3.2.2 Übermittlung an Behörden, Staatsanwaltschaften und Gerichte

Im zweiten Fall hat der Diensteanbieter gemäß § 4 Abs 3 SVN-G die Nutzerdaten des Verfassers eines bestimmten Postings an kriminalpolizeiliche Behörden, Staatsanwaltschaften und Gerichte auf deren Ersuchen hin herauszugeben und zwar zum Zweck der Aufklärung eines „konkreten Verdachts einer durch den Inhalt des Postings begangenen Straftat“³⁹. Die Aufzählung der berechtigten Stellen ist taxativ, weshalb eine Übermittlung von Nutzerdaten gemäß § 4 Abs 3 SVN-G an andere Institutionen als kriminalpolizeiliche Behörden, Staatsanwaltschaften und Gerichte, beispielsweise an andere Verwaltungsbehörden, nicht zulässig ist.

Da bei einem solchen Ersuchen auf Übermittlung von Nutzerdaten gemäß § 4 Abs 3 SVN-G (anders als bei einem Ansuchen von Dritten gemäß § 4 Abs 2 SVN-G) keine Begründung seitens der ansuchenden Stelle gefordert ist, ist auch nicht davon auszugehen, dass der Diensteanbieter prüfen muss, ob das Ersuchen zulässig ist. Eine inhaltliche Beurteilung des Ersuchens durch den Diensteanbieter kommt hier demnach nicht in Frage.

³⁷ *Rami* in Höpfel/Ratz (Hrsg), Wiener Kommentar zum StGB² Vor §§ 111–117 Rz 8 f (Stand 01.04.2021, rdb.at).

³⁸ *Reischauer* in Rummel (Hrsg), ABGB³ § 1330 ABGB Rz 1 u 1a (Stand 01.01.2004, rdb.at); RIS-Justiz RS0008985, Auch juristischen Personen kommt das Recht auf Ehre zu.

³⁹ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 4 Abs 3.

Somit hätte ein Diensteanbieter jedem Ersuchen einer gemäß § 4 Abs 3 SVN-G berechtigten Stelle Folge zu leisten und dieser die Nutzerdaten zu übermitteln.

Beim Vergleich der beiden Übermittlungstatbestände des SVN-G fällt auf, dass lediglich die Übermittlungspflicht an Dritte gemäß § 4 Abs 1 und 2 SVN-G ausschließlich auf darin taxativ angeführte Tatbestände angewendet wird, welche auch typischerweise mit der Verbreitung von Hasspostings einhergehen. Demgegenüber müssen die Nutzerdaten an kriminalpolizeiliche Behörden, Staatsanwaltschaften und Gerichte beim Verdacht jeder erdenklichen Straftat herausgegeben werden. Es handelt sich also im zweiten Fall nicht um eine Maßnahme allein zur Verfolgung von Hasskommentaren, sondern um ein uneingeschränkt anwendbares Strafverfolgungswerkzeug.

3.3 Die Registrierungs- und Identifizierungspflichten des SVN-G

Damit die Übermittlungspflichten erfüllt werden können, verpflichtet der Entwurf betroffene Diensteanbieter zunächst gemäß § 3 Abs 1 und 4 SVN-G dazu, von potentiellen Nutzern des Dienstes vorab zu verlangen, „zur Authentisierung ein Registrierungsprofil [zu - *Anm. d. Verf.*] erstellen.“⁴⁰ Erst nach erfolgreicher Registrierung dürfen Diensteanbieter Nutzern das Verfassen von Beiträgen im Forum gestatten. Eine klare Definition, was unter dem Begriff „Registrierungsprofil“ zu verstehen ist, bietet weder der Entwurf selbst noch die Erläuterungen, die Diensteanbieter müssten diese Information daher selbst aus dem Gesetzestext herleiten. Diesem ist zu entnehmen, dass gemäß § 3 Abs 4 SVN-G das Registrierungsprofil der Authentisierung eines jeden Nutzers dient.⁴¹ Demzufolge hat sich ein Nutzer „unter Angabe von Vorname, Nachname und Adresse als Poster zu registrieren. Dabei hat er einen Nutzernamen festzulegen, der im Forum als Bezeichnung für den Verfasser des Postings aufscheint. Dieser Nutzername muss nicht mit dem bürgerlichen Namen des Nutzers übereinstimmen.“⁴²

Daraus lässt sich schließen, dass ein Registrierungsprofil einen Datensatz darstellt, der jedenfalls den bürgerlichen Namen, also den Vornamen und Nachnamen sowie die Adresse eines Nutzers enthalten muss. Ob auch das vom Nutzer bei der Registrierung zu wählende

⁴⁰ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 1.

⁴¹ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 4.

⁴² ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 4.

Pseudonym, der sogenannte Nutzernamen, Bestandteil des Registrierungsprofils sein soll, lässt sich weder dem Wortlaut des § 3 Abs 4 SVN-G noch den Materialien eindeutig entnehmen, es ist aber eher davon auszugehen, dass dies nicht der Fall ist.

Wie die Erstellung des Registrierungsprofils technisch zu erfolgen hat, gibt das SVN-G nicht vor. Es ist aber anzunehmen, dass sich dies in der Praxis so gestalten würde, dass die Nutzer im Onlinedienst selbst ihre Personalien und einen Nutzernamen ihrer Wahl eingeben und der Diensteanbieter diese dann in einer internen Datenbank speichert.

3.3.1 Nutzerdaten stellen personenbezogene Daten dar

Bei den Daten, die im Rahmen der Registrierung gespeichert werden müssen, handelt es sich somit um Vorname, Nachname und Adresse eines jeden Nutzers. Zusätzlich muss auch das vom Nutzer gewählte Pseudonym (Nutzernamen) gespeichert werden, welches aber auch dem bürgerlichen Namen entsprechen kann, aber nicht muss. Bei Vorname, Nachname und Adresse handelt es sich offenkundig um personenbezogene Daten im Sinne des Art 4 Z 1 Datenschutz-Grundverordnung (DSGVO),⁴³ da diese Daten sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Ein vom Nutzer verwendetes Pseudonym stellt eine Art Kennung in Form eines Namens im Sinne des Art 4 Z 1 DSGVO dar und ist deshalb ebenfalls als personenbezogenes Datum im Sinne des Art 4 Z 1 DSGVO zu qualifizieren, da der Nutzer trotz Verwendung eines Pseudonyms anstatt seines bürgerlichen Namens jedenfalls identifizierbar ist.⁴⁴

3.3.2 Pflicht zur Überprüfung der Identität der Nutzer

Nachdem der Nutzer bei der Registrierung seine Personalien bekanntgegeben hat, trifft in der Folge den Diensteanbieter gemäß § 3 Abs 4 SVN-G die Pflicht, „für die Überprüfung der Identität des Nutzers auf der Grundlage von Dokumenten, Daten oder Informationen, die von einer glaubwürdigen und unabhängigen Quelle stammen, zu sorgen.“⁴⁵ Der

⁴³ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 2016/119, 1 idF ABl L 2021/074, 35.

⁴⁴ Art 4 Z 1 DSGVO.

⁴⁵ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 4.

Diensteanbieter muss also weitere Unterlagen oder Informationen vom Nutzer einfordern und anhand dieser verifizieren, ob die vom Nutzer angegebenen Daten richtig sind, diese also mit seiner Identität übereinstimmen.

Die Erläuterungen liefern nähere Hinweise zu dieser Identitätsüberprüfung und halten fest, dass es dem Diensteanbieter grundsätzlich freisteht, auf welche Weise er diese durchführt. Dennoch, und in diesem Zusammenhang etwas unerwartet, stellen die Erläuterungen hier aber die Möglichkeit einer Identifizierung über die Mobilfunkrufnummer des Nutzers in den Raum.⁴⁶ Die Verfasser des Entwurfs spielen hier offensichtlich auf den Identifizierungs-Dienst „Mobile Connect“ an, der von der „GSM Association“ (GSMA), der weltweit größten Interessenvertretung für Mobilfunkunternehmen, vertrieben wird. In einer früheren Fassung des Entwurfs soll die Nutzung von „Mobil Connect“ sogar noch ausdrücklich verankert gewesen sein.⁴⁷ Der Dienst „Mobile Connect“ ermöglicht, dass sich Nutzer durch Eingabe ihrer Mobilrufnummer in einen Onlinedienst einloggen können, anstatt, wie sonst meist üblich, einen Nutzernamen und ein Passwort eingeben zu müssen. Im Hintergrund überprüft dann eine Software die Identität des Nutzers, indem die vom Nutzer eingegebenen Daten (im Fall des SVN-G: Vorname, Nachname und Adresse) mit den beim Mobilfunkanbieter des Nutzers gespeicherten Stammdaten automatisch abgeglichen werden.⁴⁸

Laut den Erläuterungen zum SVN-G soll der Diensteanbieter „die für die Rechtsverfolgung notwendigen Daten“ eines Forennutzers „in Kooperation mit dem Betreiber des Telefondienstes – bei begründeten Anfragen [...] in Erfahrung bringen“⁴⁹. Diese Formulierung ist

⁴⁶ ME SVN-G, 134/ME XXVI. GP Erläut 4;

Neuwal.com, Website 13.11.2018, Transkript: Gernot Blümel bei Armin Wolf in der ZIB2
<www.neuwal.com/transkript/20181113-armin-wolf-gernot-blumel-zib2.php>
(abgefragt am 14.01.2022).

⁴⁷ *Al-Youssef*, Minister Blümels ominöse Software zur De-Anonymisierung, Website Der Standard 12.04.2019 <www.derstandard.at/2000101256631/Minister-Bluemels-ominoese-Software-zur-De-Anonymisierung> (abgefragt am 14.01.2022);

Lohninger, Das Mitmach-Internet in Gefahr: Bundesregierung will Ausweiszwang im Internet einführen, Website Epicenter.Works 10.04.2019 <www.epicenter.works/content/das-mitmach-internet-in-gefahr-bundesregierung-will-ausweiszwang-im-internet-einfuehren> (abgefragt am 14.01.2022).

⁴⁸ *Al-Youssef*, Minister Blümels ominöse Software zur De-Anonymisierung, Website Der Standard 12.04.2019 <www.derstandard.at/2000101256631/Minister-Bluemels-ominoese-Software-zur-De-Anonymisierung> (abgefragt am 14.01.2022);

Mutschler/Schmitz, So funktioniert Mobile Connect, Website Security Insider.de 30.03.2018
<www.security-insider.de/so-funktioniert-mobile-connect-a-700580> (abgefragt am 14.01.2022).

⁴⁹ ME SVN-G, 134/ME XXVI. GP Erläut 4.

wohl so zu deuten, dass der Diensteanbieter bei Verwendung eines Dienstes wie „Mobile Connect“, die Personalien seiner Forennutzer nicht selbst speichern muss, sondern diese im Bedarfsfall vom Mobilfunkanbieter des jeweiligen Nutzers erhalten soll. Das ist aber insofern fragwürdig, weil die Mobilfunkunternehmen, die mit dem SVN-G eigentlich nichts zu tun haben, hier personenbezogene Daten an andere privatrechtliche Unternehmen, nämlich die Betreiber von Diskussionsforen herausgeben müssten, was gemäß Art 6 DSGVO grundsätzlich nur mit ausdrücklicher Einwilligung des betroffenen Kunden erfolgen kann. Zudem überrascht es, dass die Verfasser des Entwurfs die bei den Mobilfunkbetreibern gespeicherten Stammdaten offensichtlich als „Daten oder Informationen, die von einer glaubwürdigen und unabhängigen Quelle stammen“⁵⁰, betrachten, wie es in § 3 Abs 4 SVN-G gefordert wird.

Möglicherweise war es die Intention der Verfasser, mit dem Hinweis auf Verfahren wie „Mobile Connect“, kritischen Stimmen den Wind aus den Segeln zu nehmen, weil es bei der Nutzung solcher Dienste unter Umständen nicht notwendig wäre, dass Diensteanbieter selbst massenhaft Namen und Adressen ihrer Nutzer speichern müssen. Die verpflichtende Nutzung eines Dienstes wie „Mobile Connect“ könnte jedoch zu zahlreichen Problemen führen. Beispielsweise hätte dies wohl zur Folge, dass damit indirekt zahlreichen Personen der Zugang zu Diskussionsforen verwehrt bleibt, beispielsweise Personen, die gar kein Handy besitzen, oder solchen, die eine Handy nutzen, welches nicht auf sie selbst angemeldet ist, sowie Personen die nur über eine ausländische Mobilrufnummer verfügen. Auch wenn die Erläuterungen diese Variante als Beispiel nennen, soll die Identifizierung der Nutzer im Wege einer „Kooperation mit dem Betreiber des Telefondienstes“⁵¹ nicht die einzige Möglichkeit sein, die Überprüfung der Nutzerdaten durchzuführen.

Wie erläutert, steht es dem Diensteanbieter frei, die Identifizierung auch „auf der Grundlage von Dokumenten, Daten oder Informationen, die von einer glaubwürdigen und unabhängigen Quelle stammen“⁵², vorzunehmen. Naheliegend wäre hier beispielsweise, dass der Diensteanbieter die Vorlage einer Ausweiskopie und des aktuellen Meldezettels des Nutzers verlangt, die diese Anforderungen an Glaubwürdigkeit und Unabhängigkeit wohl jedenfalls erfüllen sollten. Die zur Identifizierung „verwendeten Dokumente und

⁵⁰ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 4.

⁵¹ ME SVN-G, 134/ME XXVI. GP Erläut 4.

⁵² ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 4.

Informationen“⁵³, damit sind wohl übermittelte Ausweiskopien und Ähnliches gemeint, hat der Diensteanbieter nach erfolgter Überprüfung gemäß § 3 Abs 4 SVN-G unverzüglich zu löschen.⁵⁴

3.3.3 Pflicht zur periodischen Überprüfung der Nutzerdaten

In der Folge ist der Diensteanbieter gemäß § 3 Abs 5 SVN-G verpflichtet, einen bereits erfolgreich registrierten und identifizierten Nutzer bei „begründetem Verdacht auf unrichtige oder unrichtig gewordene Registrierungsangaben zum Nachweis der Richtigkeit der Angaben binnen angemessener Frist bei sonstiger Löschung des Registrierungsprofils aufzufordern“⁵⁵. Ungeklärt bleibt dabei, welche Vorkommnisse die Verfasser des Entwurfs im Sinn hatten, die in einem Diensteanbieter einen solchen „begründete[n] Verdacht auf unrichtige oder unrichtig gewordene Registrierungsangaben“⁵⁶ erwecken sollen. Es scheint, als werde hier detektivischer Spürsinn von den Diensteanbietern erwartet. Die entsprechenden Erläuterungen ergänzen hierzu noch, dass der Diensteanbieter die Richtigkeit der Daten aber nicht ausschließlich in solchen Verdachtsfällen, sondern diese darüber hinaus ganz generell „routinemäßig periodisch“⁵⁷ zu überprüfen hat, jedoch ohne Details für die konkrete Durchführung dieser regelmäßigen Überprüfung zu nennen, was eine gesetzeskonforme Umsetzung dieser Pflicht für die Diensteanbieter wohl schwierig gestalten dürfte.

3.3.4 Pflicht zur Überprüfung der regelmäßigen Aktivität der Nutzer

Des Weiteren muss der Diensteanbieter gemäß § 3 Abs 6 Z 3 SVN-G zusätzlich laufend überprüfen, ob ein registrierter Nutzer im Forum auch tatsächlich regelmäßig aktiv ist. Liegt die letzte Nutzung des Forums mehr als ein Jahr zurück, so trifft den Diensteanbieter auch in diesem Fall die Pflicht, das Registrierungsprofil dieses Nutzers zu löschen. Der Entwurf sieht vor, dass eine solche Inaktivität von mehr als einem Jahr vom Diensteanbieter

⁵³ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 4.

⁵⁴ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 4.

⁵⁵ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 5.

⁵⁶ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 5.

⁵⁷ ME SVN-G, 134/ME XXVI. GP Erläut 5.

„im Rahmen von routinemäßig periodisch vorgenommenen Überprüfungsvorgängen“⁵⁸ festzustellen ist. Auch wie diese periodischen Überprüfungen konkret zu erfolgen haben, gibt das SVN-G nicht vor. Technisch umgesetzt würde das aber bedeuten, dass der Diensteanbieter bei jedem einzelnen Einloggsvorgang eines Nutzers das aktuelle Datum und eventuell auch die Uhrzeit, also einen sogenannten Zeitstempel, speichern muss. Denn schließlich kann der Diensteanbieter nur auf diese Weise nachverfolgen, ob seit der jeweils letzten Aktivität des Nutzers bereits mehr als ein Jahr verstrichen ist. Daraus folgt, dass der Diensteanbieter mit diesen Zeitstempeln unweigerlich eine weitere Datenkategorie zu speichern hat, welche zwar nicht ausdrücklich im SVN-G erwähnt wird, die aber technisch bedingt unvermeidbar ist. Aus den gesammelten Zeitstempeln würde sich eine Art Nutzungsprofil eines jeden registrierten Nutzers ergeben, anhand dessen sich die Zeitpunkte und Zeiträume, in denen dieser im Forum aktiv war, exakt nachverfolgen ließen. Verstöße des Diensteanbieters gegen die Überprüfung auf Inaktivität gemäß § 3 Abs 6 Z 3 SVN-G werden gemäß § 7 Abs 1 Z 4 SVN-G mit „Geldbuße bis zu 500.000 Euro, im Wiederholungsfall bis zu 1.000.000 Euro“⁵⁹ geahndet. Angesichts dieser hohen Strafen wird man davon ausgehen können, dass Diensteanbieter sich tunlichst bemühen würden, für jeden Nutzer ein möglichst exaktes und lückenloses Profil, welches die zeitliche Nutzung wiedergibt, zu erstellen.

Die zu speichernden Zeitangaben, also Datum und Uhrzeit, sind für sich allein betrachtet noch keine personenbezogenen Daten. Allerdings muss beim Diensteanbieter eine Zuordnung in Form einer Verknüpfung zu den personenbezogenen Daten des jeweiligen Nutzers vorgenommen werden, was eine Verarbeitung gemäß Art 4 Z 2 DSGVO darstellt und zur Identifizierbarkeit des Nutzers führt.

3.4 Pflicht zur Speicherung und Übermittlung von Postinginhalten

Das SVN-G belässt es aber nicht dabei, die Speicherung von Vorname, Nachname, Adresse, Pseudonym und der Zeitstempel sämtlicher Nutzer anzuordnen. Es verpflichtet die Diensteanbieter darüber hinaus gemäß § 4 Abs 4 SVN-G dazu, von jedem Posting, welches zum Anlass eines Auskunftsverlangens wird, „eine Aufzeichnung herzustellen, die eine

⁵⁸ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 6 Z 3.

⁵⁹ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 7 Abs 1 und Abs 1 Z 4.

vollständige und originalgetreue Wiedergabe ermöglicht.“⁶⁰ Diese Aufzeichnungspflicht kann nur so zu verstehen sein, dass der Diensteanbieter das betreffende Posting bzw dessen Inhalt zu speichern hat. Der Diensteanbieter hat in der Folge diese Aufzeichnung des Postings an den Ansuchenden zu übermitteln. Kann der Diensteanbieter keine Aufzeichnung eines bestimmten Postings herausgeben, dann stellt dies einen Verstoß gegen eine der in § 4 SVN-G geregelten Übermittlungspflichten dar. § 7 Abs 1 Z 5 SVN-G ordnet an, dass über einen Diensteanbieter, wenn dieser „einer der in § 4 geregelten Pflichten zur Übermittlung von Daten nicht entspricht“⁶¹, eine der angeführten, mitunter beachtlichen Geldbußen zu verhängen ist, die „je nach Schwere des Vergehens [...] bis zu 500.000 Euro, im Wiederholungsfall bis zu 1.000.000 Euro“⁶² betragen können.

Das SVN-G sieht dabei vor, dass solche Aufzeichnungen von Postings beim Vorliegen von „begründeten Hinweisen, dass durch den Inhalt eines Postings der objektive Tatbestand der üblen Nachrede oder der Beleidigung hergestellt worden sein könnte oder dass der Inhalt sonst den konkreten Verdacht einer Straftat begründen könnte“⁶³, anzufertigen sind.

Hier ist fraglich, wie der Diensteanbieter feststellen soll, dass solche „begründeten Hinweise“ auf die Verwirklichung der genannten Tatbestände bzw Straftaten vorliegen. Tatsächlich wird er diese „begründeten Hinweise“ wohl erst durch ein Ersuchen um Übermittlung der Nutzerdaten gemäß SVN-G erhalten. Spätestens dann muss der Diensteanbieter eine solche Aufzeichnung eines Postings herstellen.

3.4.1 Postings stellen personenbezogene Daten dar

Da die Diensteanbieter damit verpflichtet sind, auch Postings zu verarbeiten, um die Aufzeichnungspflicht zu erfüllen und auch den Inhalt von Postings zu analysieren, um beurteilen zu können, ob Übermittlungsersuchen zulässig sind, ist auch die datenschutzrechtliche Qualifikation der Postings in den vom SVN-G umfassten Onlineforen zu untersuchen. Ob die von einem Nutzer in einem Forum verfassten und veröffentlichten Kommentare personenbezogene Daten im Sinne des Art 4 Z 1 DSGVO darstellen, hängt in erster Line davon ab, ob die Postings sich auf die Person des Verfassers zurückführen

⁶⁰ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 4 Abs 4.

⁶¹ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 7 Abs 1 Z 5.

⁶² ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 7 Abs 1.

⁶³ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 4 Abs 4.

lassen. Die österreichische Datenschutzbehörde (DSB) hat dies zuletzt im Bescheid DSB 13.8.2018, D123.077/0003-DSB/2018 konkretisiert: Legt ein Forennutzer gegenüber dem Diensteanbieter seinen vollständigen Namen offen, bewirkt dies, dass sich die Postings bzw der Inhalt der Postings auf diesen Nutzer zurückführen lassen und dieser somit gegenüber dem Diensteanbieter identifiziert ist.⁶⁴ Im Anwendungsbereich des SVN-G ist dies nach erfolgter Registrierung eines Nutzers definitiv gegeben, weshalb die Postings eines registrierten Nutzers auch personenbezogene Daten im Sinne des Art 4 Z 1 DSGVO darstellen.

Abgesehen vom konkreten Fall des SVN-G ist davon auszugehen, dass auch bei jeder anderen Variante einer Klarnamenpflicht bzw verpflichtenden namentlichen Registrierung und Identifizierung die Zurückführbarkeit eines Postinginhalts auf den Verfasser gegeben sein wird. Wird einem Diensteanbieter jedoch keine Form von Klarnamen- oder Identifizierungspflicht auferlegt, so können Postinginhalte nicht auf den konkreten Verfasser zurückgeführt werden, da es dann an der Identifizierbarkeit mangelt, vorausgesetzt, der Verfasser hat nicht freiwillig seinen bürgerlichen Namen als Nutzernamen verwendet. Bei den Postings handelt es sich dann um sogenannte anonyme Daten, die nicht in den Anwendungsbereich des Datenschutzgesetzes (DSG)⁶⁵ bzw der DSGVO fallen.⁶⁶

Auch wenn in einem Diskussionsforum keine Form von Identifizierungspflicht vorgesehen ist, und die Nutzer daher tatsächlich anonym posten können, ist es aber dennoch möglich, dass einzelne Postings trotzdem personenbezogene Daten im Sinne der DSGVO darstellen, nämlich dann, wenn der Verfasser im Inhalt des Postings Informationen oder auch Werturteile über eine andere Person veröffentlicht, anhand derer diese Person identifiziert werden kann.⁶⁷ Wenn nun also in einem anonym verfassten Posting beispielsweise der Namen oder die Wohnadresse einer Person genannt wird, dann ist dieses Posting als personenbezogenes Datum im Sinne des Art 4 Z 1 DSGVO zu qualifizieren.⁶⁸

⁶⁴ DSB 13.8.2018, D123.077/0003-DSB/2018.

⁶⁵ Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), BGBl I 165/1999 idF I 14/2019.

⁶⁶ Hödl in Knyrim (Hrsg), Der DatKomm. Praxiskommentar zum Datenschutzrecht - DSGVO und DSG, Art 4 DSGVO RZ 17 (Stand 01.12.2018, rdb.at).

⁶⁷ Hödl in Knyrim (Hrsg), Der DatKomm. Praxiskommentar zum Datenschutzrecht - DSGVO und DSG, Art 4 DSGVO RZ 9 (Stand 01.12.2018, rdb.at).

⁶⁸ Koukal, Kritische Äußerungen auf einem Onlineforum als Datenverwendung iS des DSG - personenbezogene Daten - Untersagung - Widerspruch (§ 28 Abs 2 DSG), MR 2009, 306 (308).

Je nach Art des Inhalts von Postings kann es sich dabei auch um sensible personenbezogene Daten handeln. Diese in Art 9 Abs 1 DSGVO als „besondere Kategorien personenbezogener Daten“⁶⁹ bezeichneten Daten sind definiert als „personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, [...] Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person“⁷⁰. Art 9 Abs 1 DSGVO untersagt die Verarbeitung solcher sensiblen personenbezogenen Daten grundsätzlich, sieht in den auf Absatz 1 folgenden Absätzen jedoch Ausnahmen vor.

Da Diskussionsforen im Internet dem freien Meinungs Austausch dienen, entscheiden dabei allein die Nutzer, welche Informationen sie in ihren Postings kundtun. Daher sind auch praktisch alle der in Art 9 Abs 1 DSGVO angeführten Datenkategorien denkbarer Inhalt von Kommentaren. Gibt ein Nutzer in einem seiner Postings eine der angeführten sensiblen Informationen von sich preis, hat dies zur Folge, dass das betreffende Posting damit zu einem sensiblen Datum im Sinne des Art 9 Abs 1 DSGVO wird. Darüber hinaus existieren auch zahlreiche Internetforen, die eigens zur Diskussion solcher sensibler Themenbereiche, wie etwa Sexualität oder psychische Krankheiten, vorgesehen sind.

3.4.2 Ist die Löschung von Postings dennoch erlaubt?

Im Zusammenhang mit der durch § 4 Abs 4 SVN-G verankerten Aufzeichnungs- und Übermittlungspflicht betreffend Postings stellen sich diverse Fragen.

Ungewiss ist zum einen, ob der Diensteanbieter, obwohl er offensichtlich jederzeit Aufzeichnungen konkreter Postings anfertigen und herausgeben können muss, dennoch eine Funktion in seinem Forum anbieten darf, mittels der die Nutzer einzelne ihrer selbstverfassten Postings löschen dürfen. Ebenso fraglich ist, ob der Diensteanbieter selbst Postings löschen darf, etwa dann, wenn ein Nutzer die Entfernung eines seiner Postings vom Diensteanbieter fordert. Beides ist seit jeher in Internetforen gängige Praxis. Zudem ist es in vielen Diskussionsforen üblich, dass Moderatoren selbsttätig Kommentare löschen, die

⁶⁹ Art 9 Abs 1 DSGVO.

⁷⁰ Art 9 Abs 1 DSGVO.

gegen die Forenrichtlinien des jeweiligen Dienstes verstoßen.⁷¹

Würde aber nun ein berechtigter Antragsteller gemäß § 4 Abs 4 SVN-G die Herausgabe eines bestimmten Postings verlangen, dann könnte der Diensteanbieter dieser Übermittlungspflicht nicht mehr nachkommen, wenn jenes Posting bereits vor der Antragstellung des Berechtigten durch einen Nutzer oder den Diensteanbieter selbst gelöscht worden ist. Der Entwurf nimmt zur Frage, ob die Löschung von Postings in bestimmten Fällen zulässig ist, keine Stellung. Insofern werden die Diensteanbieter im Unklaren gelassen, wie tiefgreifend die Aufzeichnungs- und Herausgabepflicht betreffend Postings die Gestaltungsfreiheit der Diensteanbieter hinsichtlich des technischen Designs ihrer Foren einschränkt.

Nachdem die Nichtbefolgung der Herausgabepflicht des § 4 Abs 4 SVN-G aber nach der Systematik des Gesetzesentwurfs einen Verstoß darstellt, der grundsätzlich eine Geldstrafe für den Diensteanbieter nach sich ziehen würde,⁷² könnte die Gefahr bestehen, dass Diensteanbieter diese Bestimmung zu restriktiv auslegen und möglicherweise sogar dazu übergehen könnten, den Nutzern keine Löschmöglichkeit mehr einzuräumen und stattdessen tatsächlich sämtliche Postings auf unbegrenzte Zeit gespeichert zu belassen, um stets die Pflicht zur Herausgabe von Aufzeichnungen der Postings erfüllen zu können.

Würde man die Verpflichtung des § 4 Abs 4 SVN-G auf diese Weise interpretieren, dann würde dies jedoch eine nur schwer nachvollziehbare, gänzliche Abkehr von der gewohnten Praxis bedeuten. Denn derzeit ist es üblich, öffentlich zugängliche Hasspostings so schnell wie möglich zu löschen, schließlich handelt es sich dabei zumeist um Persönlichkeitsverletzungen und Herabwürdigungen der betroffenen Personen. Dass der Fokus sinnvollerweise auf die Entfernung von Hasskommentaren zu legen ist, wurde zuletzt auch durch das richtungsweisende Urteil des Europäischen Gerichtshofs (EuGH) vom 03.10.2019 in der Rechtssache C-18/18 (*Glawischnig-Piesczek*) verdeutlicht, das darüber hinaus die Diensteanbieter in der Pflicht sieht, auch gleichlautende Kommentare und selbst sinngleiche Postings von ihren Plattformen zu löschen und dies sogar weltweit.⁷³

⁷¹ Der Standard, Website 04.01.2019, Dem Hass im Netz keine Chance: Wie DER STANDARD sein Forum moderiert <www.derstandard.at/story/2000095396987/dem-hass-keine-chance-wie-der-standard-sein-forum-moderiert> (abgefragt am 14.01.2022);

Burger, Sch(m)utz im Netz. Warum wir digitale Masken brauchen (2021) 81 ff.

⁷² ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 7 Abs 1 Z 5.

⁷³ EuGH 03.10.2019, C-18/18 (*Glawischnig-Piesczek*);

Lehofer, Hass im Netz und gedruckt: europäische Gerichte, österreichische Fälle, ÖJZ 2019/112, 893.

Die Bedeutung der raschen Entfernung von rechtswidrigen Postings hat zuvor auch bereits der Europäische Gerichtshof für Menschenrechte (EGMR) im Urteil vom 16.06.2015 64569/09 (*Delfi AS gg Estland*)⁷⁴ unterstrichen. Diesem Urteil nach können Plattformbetreiber beim Vorliegen bestimmter Voraussetzungen und einer entsprechenden nationalen gesetzlichen Grundlage zur umgehenden Löschung von anonymen Hasspostings verpflichtet werden. Dies gilt insbesondere dann, wenn der Plattformbetreiber einen kommerziellen Vorteil aus einem für Nutzer eingerichteten Kommentarbereich zieht. Nach Ansicht des EGMR stellt eine solche Pflicht zur Löschung von Hasspostings unter den im Fall *Delfi* vorgelegenen Voraussetzungen auch keine Verletzung des Grundrechts auf freie Meinungsäußerung (Art 10 EMRK) dar.⁷⁵

In Österreich besteht gemäß der Bestimmung des § 18 Abs 1 ECG keine allgemeine Überwachungspflicht für Forenbetreiber, diese müssen also nicht aktiv nach rechtswidrigen Postings Ausschau halten, sondern erst nach einem entsprechenden Hinweis tätig werden. Die Haftung für den Inhalt eines rechtswidrigen Postings liegt somit grundsätzlich beim Nutzer, der dieses verfasst hat. Der Forenbetreiber würde erst dann haften, wenn er Kenntnis von einem rechtswidrigen Nutzerkommentar in seinem Forum erlangt, aber nicht dagegen vorgeht.⁷⁶

Tatsächlich ist davon auszugehen, dass die Pflicht zur Anfertigung und Herausgabe von Aufzeichnungen von Postings durch den Diensteanbieter⁷⁷ eine Beweissicherungsmaßnahme darstellt. Mit der Aufzeichnung eines Postings durch den Diensteanbieter soll offenbar belegt werden, dass ein bestimmtes Posting tatsächlich online war, sowie die Zeit nachgewiesen werden, zu der dieses im Forum abrufbar war, also Umstände, die beispielsweise durch einen vom Betroffenen angefertigten bloßen Screenshot nicht zwingend bewiesen werden könnten. Es war vermutlich das Ansinnen der Verfasser des Entwurfs, einem Betroffenen die Verfolgung des Täters so einfach wie möglich zu machen und eventuelle Beweisschwierigkeiten zu vermeiden.

⁷⁴ EGMR 16.06.2015, 64569/09 (GK) (*Delfi AS gg Estland*).

⁷⁵ *Fötschl*, Die Entscheidung *Delfi* des EGMR: Der Einfluss der Grundrechte auf das Host-Provider-Haftungsprivileg, *ecolx* 2015, 827 ff.

⁷⁶ *Zankl*, E-Commerce-Gesetz. Kommentar² (2016) § 18 Rz 335 ff.

⁷⁷ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 4 Abs 4.

Das SVN-G sieht vor, dass eine Aufzeichnung eines Postings nur nach Einlangen von „begründeten Hinweisen“⁷⁸ auf eine durch das Posting bewirkte Rechtsverletzung anzufertigen ist. Es muss aber dennoch erlaubt sein, Postings vor dem Einlangen eines solchen Hinweises zu ändern oder zu löschen, da dies sonst im Widerspruch zum Recht der Nutzer auf Löschung der eigenen personenbezogenen Daten stehen würde.⁷⁹ Geht ein Hinweis zu einem verdächtigen Posting ein, das zu diesem Zeitpunkt aber bereits aufgrund von Änderung oder Löschung nicht mehr online ist, dann muss der Diensteanbieter auch keine Aufzeichnung anfertigen und herausgegeben, denn das wäre dann schließlich auch gar nicht mehr möglich. Dem Diensteanbieter kann in diesem Fall folgerichtig auch keine Geldbuße auferlegt werden.

Die Bestimmung des § 4 Abs 4 SVN-G ist also nicht dahingehend zu interpretieren, dass sämtliche Postings dauerhaft gespeichert werden müssen, um stets Aufzeichnungen aller Postings herausgeben zu können und so drohenden Geldbußen zu entgehen. Leider fehlt sowohl dem Entwurf des SVN-G als auch den Erläuterungen hier die nötige Klarheit.

3.4.3 Anwendung des Medienprivilegs auf Postings

Auf Internetforen sind prinzipiell die allgemeinen datenschutzrechtlichen Grundsätze betreffend das Recht auf Löschung anzuwenden. Wenn es sich bei Postings um personenbezogene Daten handelt, so hat der jeweils Betroffene, also entweder der Urheber des Postings selbst, oder jene Person, deren personenbezogene Daten im Inhalt des Postings veröffentlicht wurden, das Recht, vom Forenbetreiber zu verlangen, gemäß Art 17 DSGVO die Löschung unverzüglich durchzuführen.⁸⁰ Eine Ausnahme von diesem Grundsatz wird aber durch das sogenannte Medienprivileg (oder auch Informationsfreiheitsprivileg) begründet: Handelt es sich bei dem Betreiber eines Diskussionsforums um einen Medieninhaber oder Mediendienst im Sinne des Mediengesetzes,⁸¹ und erfolgt die Verar-

⁷⁸ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 4 Abs 4.

⁷⁹ Art 17 DSGVO;

Haidinger in Knyrim (Hrsg), Der DatKomm. Praxiskommentar zum Datenschutzrecht - DSGVO und DSG, Art 17 DSGVO RZ 61 u 65 (Stand 01.10.2018, rdb.at).

⁸⁰ *Haidinger* in Knyrim (Hrsg), Der DatKomm. Praxiskommentar zum Datenschutzrecht - DSGVO und DSG, Art 17 DSGVO RZ 61 u 65 (Stand 01.10.2018, rdb.at).

⁸¹ Bundesgesetz vom 12. Juni 1981 über die Presse und andere publizistische Medien (Mediengesetz – MedienG), BGBl 314/1981 idF I 32/2018.

beitung der personenbezogenen Daten im Forum zu journalistischen Zwecken, so kommt dem Betreiber dieses Dienstes das Medienprivileg des § 9 Abs 1 DSG zugute. Diese Bestimmung sieht vor, dass weite Bereiche des DSG und der DSGVO auf eine solche Datenverarbeitung zu journalistischen Zwecken nicht anwendbar sind.⁸² Unter anderem entfällt das in Art 17 DSGVO verankerte Recht eines Forennutzers auf Löschung seiner personenbezogenen Daten, was bedeutet, dass der Nutzer in diesem Fall kein Recht auf Löschung eines seiner Postings hätte.

Erste Vorfrage für die Beurteilung, ob einem Forenbetreiber betreffend ein bestimmtes Posting das Medienprivileg zukommt, ist zunächst stets, ob es sich bei den im betroffenen Posting enthaltenen Informationen überhaupt um personenbezogene Daten im Sinne des Art 4 Z 4 DSGVO handelt. Wie bereits dargestellt, ist ein Posting jedenfalls dann als personenbezogenes Datum zu qualifizieren, wenn sich der Verfasser gegenüber dem Diensteanbieter identifiziert hat und das Posting bzw der Inhalt des Postings sich dadurch auf den Verfasser zurückführen lässt.⁸³ Dies wäre unter Anwendung von Klarnamen- bzw Identifizierungspflichten wie dem SVN-G stets der Fall. In einem zweiten Schritt ist dann zu beurteilen, ob die Verarbeitung dieser personenbezogenen Daten, also die Speicherung der Kommentare im Forum, tatsächlich zu journalistischen Zwecke erfolgt ist. Der EuGH hat in seiner Entscheidung vom 16.12.2008, C-73/07 (*Satakunnan Markkinapörssi und Satamedia*), verdeutlicht, dass Datenverarbeitungsvorgänge dann allein zu journalistischen Zwecken erfolgen, „wenn sie ausschließlich zum Ziel haben, Informationen, Meinungen oder Ideen in der Öffentlichkeit zu verbreiten“⁸⁴. Zudem hat der EuGH in diesem Urteil festgehalten, dass solche journalistischen Tätigkeiten nicht nur Medienunternehmen und Berufsjournalisten vorbehalten sind.⁸⁵ Vielmehr kann jedermann eine journalistische Tätigkeit ausüben, wenn er damit das Ziel verfolgt, der Öffentlichkeit Informationen zukommen zu lassen. Man spricht dann vom sogenannten Bürgerjournalismus.⁸⁶ Somit können auch Postings in Internetforen, beispielsweise die Leserkommentare im Forumsbereich unter einem Artikel einer Online-Zeitung, als Bürgerjournalismus

⁸² § 9 Abs 1 DSG.

⁸³ DSB 13.8.2018, D123.077/0003-DSB/2018.

⁸⁴ EuGH 16.12.2008, C-73/07 (*Satakunnan Markkinapörssi und Satamedia*), Rz 62;
DSB 13.8.2018, D123.077/0003-DSB/2018.

⁸⁵ EuGH 16.12.2008, C-73/07 (*Satakunnan Markkinapörssi und Satamedia*), Rz 61;
DSB 13.8.2018, D123.077/0003-DSB/2018.

⁸⁶ *Mersch*, Mediengesetzliche Eckpunkte für den Bürgerjournalismus, in Berka/Holoubek/Leitl-Staudinger (Hrsg), BürgerInnen im Web, REM Bd 14 (2016) 17 (35 f).

qualifiziert werden.⁸⁷ Jedoch ist andererseits nicht jede Veröffentlichung von Kommentaren durch Bürger im Internet als Journalismus zu qualifizieren, etwa wenn auch andere Absichten als die reine Verbreitung von Information mitspielen.⁸⁸ Die DSB folgt dieser weiten Auslegung des Journalismusbegriffs durch den EuGH und weist darauf hin, dass dies auch mit den Erwägungsgründen der DSGVO im Einklang stehe.⁸⁹

Kommt einem Forenbetreiber als Medieninhaber oder -betreiber nun bezüglich eines bestimmten Postings das Medienprivileg zu, dann hat er die Möglichkeit, selbst zu entscheiden, ob er dem Löschbegehren eines Nutzers betreffend dieses Posting nachkommt. Der Diensteanbieter kann die Löschung aber auch mit Verweis auf die privilegierte journalistische Bedeutung des Postings für den Kontext des Onlineforums ablehnen.⁹⁰

3.5 Löschpflichten betreffend das Registrierungsprofil

Weitere Unsicherheiten bringt § 3 Abs 6 SVN-G mit sich. Gemäß dieser Bestimmung hat ein Diensteanbieter das Registrierungsprofil eines Nutzers in drei taxativ aufgezählten Fällen zu löschen, und zwar auf Verlangen des Nutzers, bei Abmeldung des Nutzers vom Onlinedienst und bei festgestellter Inaktivität des Nutzers von mehr als einem Jahr.⁹¹ Fraglich bleibt dabei, welche Auswirkungen eine solche verpflichtende Löschung des Registrierungsprofils haben soll und welche Daten dabei tatsächlich gelöscht werden müssen.

Wie bereits erläutert, ist entsprechend des Wortlauts des § 3 Abs 4 SVN-G davon auszugehen, dass das Registrierungsprofil einen Datensatz darstellt, in dem der Diensteanbieter Vorname, Nachname und Adresse eines Nutzers zu speichern hat. Das vom Nutzer zu wählende Pseudonym, der sogenannte Nutzernamen, scheint dabei eher nicht Bestandteil des Registrierungsprofils zu sein.⁹² Falls der Nutzernamen im Anwendungsfall des SVN-G,

⁸⁷ DSB 13.8.2018, D123.077/0003-DSB/2018.

⁸⁸ EuGH 14.02.2019, C-345/17 (*Buivids*), Rz 62;
Thiele, EuGH: Grenzen des Medienprivilegs für den Bürgerjournalismus, *jusIT* 2019/27, 82 (82).

⁸⁹ DSB 13.8.2018, D123.077/0003-DSB/2018;
EuGH 16.12.2008, C-73/07 (*Satakunnan Markkinapörssi und Satamedia*), Rz 61;
Thiele, DSB: Medienprivileg für Online-Forum und Postings, *jusIT* 2018/87, 250 (250).

⁹⁰ DSB 13.8.2018, D123.077/0003-DSB/2018.

⁹¹ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 6.

⁹² ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 4.

anders als angenommen, aber ebenfalls zum Registrierungsprofil zählen soll, ist zu erwarten, dass der Diensteanbieter im Fall einer verpflichtenden Löschung eines Registrierungsprofils auch bei jedem Posting des betreffenden Nutzers zumindest den Nutzernamen entfernen, also löschen muss, was einer Anonymisierung im Sinne der Erwägungsgründe zur DSGVO entsprechen würde.⁹³ Ist der Nutzernamen hingegen nicht als Bestandteil des Registrierungsprofils zu sehen, muss dieser nach Löschung des Registrierungsprofils bei den einzelnen Postings auch nicht entfernt werden.

Nach erfolgter Löschung des Registrierungsprofils und der darin enthaltenen Personalien wäre die Offenlegung der Identität des Nutzers unter Anwendung der Auskunftspflichten des SVN-G durch den Diensteanbieter nicht mehr möglich, denn schließlich würden dem Diensteanbieter dann Name und Adresse des Nutzers, aufgrund der vorangegangenen Löschung dieser Daten, nicht mehr vorliegen. Auch wenn der Entwurf des SVN-G diese Rechtsfolge nicht explizit nennt, kann es folgerichtig nur so sein, dass eine verpflichtende Löschung des Registrierungsprofils gemäß § 3 Abs 6 SVN-G den Diensteanbieter jedenfalls von den Übermittlungspflichten gemäß § 4 Abs 1 bis 3 SVN-G befreit, also den Pflichten zur Übermittlung von Vorname, Nachname und Adresse eines bestimmten Nutzers an auskunftsberechtigte Gerichte, Behörden oder Dritte,⁹⁴ da diese Pflichten nach Löschung der Registrierungsdaten ja auch gar nicht mehr erfüllbar wären.

Weniger klar ist jedoch, ob die Löschung eines Registrierungsprofils eines Nutzers auch von der Anwendung der übrigen Bestimmungen und Verpflichtungen des SVN-G befreit, oder ob diese ganz oder teilweise weiterhin auf diesen gelöschten Nutzer anzuwenden sind. Unter anderem stellt sich diese Frage hinsichtlich der Postings von Nutzern, deren Registrierungsprofil entsprechend den Bestimmungen des SVN-G gelöscht wurde. Da die Postings nicht zum Registrierungsprofil zählen, blieben diese nach dessen Löschung weiter im Forum bestehen. Es kann also durchaus der Fall eintreten, dass sich jemand durch ein Posting eines bereits gelöschten Nutzers in seinen Rechten verletzt sehen und daher die Herausgabe einer Aufzeichnung dieses Postings unter Berufung auf § 4 Abs 4 SVN-G verlangen könnte. Ob die Löschung des Registrierungsprofils den Diensteanbieter auch von dieser Pflicht befreit, also der Pflicht Aufzeichnungen von Postings an Gerichte, Behörden oder Dritte zu übermitteln, lassen Gesetzestext und Materialien zum SVN-G aber leider

⁹³ Bergauer/Jahnel (Hrsg), DSGVO und DSG. Das neue Datenschutzrecht³ (2018) 35, Art 4 DSGVO, Erwägungsgrund 26.

⁹⁴ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 4 Abs 1 bis 3.

unbeantwortet. Da Verstöße gegen die Aufzeichnungs- und Herausgabepflicht für Postings aber gemäß § 7 Abs 1 Z 5 SVN-G mit unter Umständen beachtlichen Geldbußen geahndet werden,⁹⁵ hätte der Diensteanbieter angesichts dieser Ungewissheit keine andere Wahl, als zur Sicherheit auch nach Löschung eines Registrierungsprofils eines Nutzers dessen Postings gespeichert zu belassen und diese bei Anträgen auf Übermittlung gemäß SVN-G auch herauszugeben, vorausgesetzt der ehemalige Nutzer hat nicht ausdrücklich die Löschung seiner Postings vom Diensteanbieter verlangt. Die Ausfolgung von Postings wäre freilich nur noch ohne Übermittlung der Identitätsdaten des Verfassers möglich, weil dem Diensteanbieter dann Name und Adresse gar nicht mehr bekannt wären.

3.6 Verbot der Verknüpfung von Nutzerdaten

Das SVN-G bestimmt mit § 4 Abs 4 letzter Satz, dass „[b]eim Diensteanbieter [...] keine Verknüpfung zwischen der Identität eines Posters und dem Inhalt eines Postings vorgenommen werden [darf - *Anm. d. Verf.*]“.⁹⁶ Es bleibt offen, wie dieses Verbot zu verstehen ist und was damit bezweckt werden soll. Auch die Erläuterungen klären hierzu nicht auf, da sie im Grunde lediglich den Wortlaut des Entwurfs wiederholen.⁹⁷ Möglicherweise wollten die Verfasser des Entwurfs durch diese Formulierung datenschutzrechtlichen Problemen aus dem Weg gehen, die etwa dann denkbar wären, wenn man die Verknüpfung von Identität und Postinginhalt als sogenanntes Profiling im Sinne des Art 4 Z 4 DSGVO qualifizieren würde, also etwa einer Auswertung der oft Informationen über den höchstpersönlichen Lebensbereich enthaltenden Postinginhalte durch Diensteanbieter zur Erstellung von Persönlichkeitsanalysen.⁹⁸ Dann könnte gemäß Art 35 Abs 2 lit a DSGVO eine Datenschutz-Folgenabschätzung notwendig sein.⁹⁹

⁹⁵ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 7 Abs 1 Z 5.

⁹⁶ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 4 Abs 4 letzter Satz.

⁹⁷ ME SVN-G, 134/ME XXVI. GP Erläut 5.

⁹⁸ Hödl in Knyrim (Hrsg), Der DatKomm. Praxiskommentar zum Datenschutzrecht - DSGVO und DSG, Art 4 DSGVO RZ 51 (Stand 01.12.2018, rdb.at).

⁹⁹ Hödl in Knyrim (Hrsg), Der DatKomm. Praxiskommentar zum Datenschutzrecht - DSGVO und DSG, Art 4 DSGVO RZ 56 (Stand 01.12.2018, rdb.at);
Art 35 Abs 2 lit a DSGVO.

3.7 Ergebnis der Analyse des Gesetzestextes des SVN-G

Die Analyse des Normtextes und der Materialien zum Entwurf führt zum Ergebnis, dass erhebliche Unklarheiten vorliegen, was die korrekte Auslegung einzelner Bestimmungen des SVN-G und der darin angeordneten Pflichten sowie der verbleibenden Rechte der Forennutzer und Diensteanbieter anbelangt. Dies kann unweigerlich zu diversen Problemen führen, die die Anwendung des SVN-G in der Praxis in manchen Teilen schwierig gestalten würden. So enthält der Entwurf einerseits eine Reihe von spezifischen Verpflichtungen für die Diensteanbieter, erläutert jedoch teilweise nicht, welche konkreten Rechtsfolgen daraus resultieren sollen. Bei falscher Auslegung droht den Diensteanbietern, dass sie dadurch Verstöße insbesondere gegen Datenschutzrecht verursachen, zusätzlich sind sie stets mit der Gefahr der hohen Strafzahlungen des SVN-G konfrontiert.

3.7.1 Einschränkung auf bestimmte Kategorien von Internetforen

Ebenfalls kritisch zu sehen, ist die Eingrenzung des Anwendungsbereichs des SVN-G auf ausschließlich solche Foren, die bestimmte Größenanforderungen insbesondere betreffend Nutzerzahlen und Jahresumsatz erfüllen. Dies kann den Eindruck einer Ungleichbehandlung der verschiedenen Forenanbieter erwecken, die sich auch durch die diesbezüglichen Erläuterungen in den Materialien zum Entwurf nicht nachvollziehen lässt. Diese Eingrenzung scheint zu ignorieren, dass sich das Phänomen „Hass im Netz“ nicht allein auf solche Foren beschränkt, die diese Erheblichkeitsschwellen des SVN-G übersteigen, also etwa 100.000 registrierte Nutzer.

Dies führt zu dem unbefriedigenden Ergebnis, dass beispielsweise das Forum der Tageszeitung „Der Standard“, dessen Betreiber bemüht sind, durch den Einsatz von Moderatoren die Diskussionskultur im Forum zu wahren,¹⁰⁰ sehr wohl dem SVN-G unterliegen würde, während das deutlich kleinere Forum der FPÖ-nahen Plattform „unzensuriert.at“, der oft

¹⁰⁰ Burger, Sch(m)utz im Netz. Warum wir digitale Masken brauchen (2021) 84 ff;

Der Standard, Website 04.01.2019, Dem Hass im Netz keine Chance: Wie DER STANDARD sein Forum moderiert <www.derstandard.at/story/2000095396987/dem-hass-keine-chance-wie-der-standard-sein-forum-moderiert> (abgefragt am 14.01.2022).

nachgesagt wird, nicht gegen Hasskommentare vorzugehen, nicht betroffen wäre.¹⁰¹

Wenn der Gesetzgeber keine schlüssige Begründung für die gewählten Größenanforderungen an Foren bietet, läuft er Gefahr, dass im schlimmsten Fall der Anschein entsteht, dass das Gesetz bewusst auf die Onlineangebote bestimmter Anbieter zugeschnitten sein könnte, eventuell sogar aus politischem Kalkül.

Die in den Erläuterungen getroffene Erklärung, dass die wirtschaftliche Leistungsfähigkeit ausschlaggebend dafür ist, dass nur Foren mit entsprechender Größe die Umsetzung der Verpflichtungen des SVN-G zumutbar sei, lässt sich beispielsweise durch einen Verweis auf den vergleichbaren Fall der gesetzlich verpflichtenden Übermittlung von Kundendaten durch Telekomunternehmen an Strafverfolgungsbehörden entkräften.¹⁰² Hierfür hat der Gesetzgeber nämlich einen Kostenersatz für die betroffenen Telekomanbieter vorgesehen, um auch kleinere Unternehmen durch diese Mitwirkungspflicht nicht wirtschaftlich zu belasten.¹⁰³ Ein Ersatz für die laufenden Aufwendungen der Diensteanbieter hätte auch im Fall des SVN-G eine sinnvolle Lösung darstellen können.

Auch dass die bei Verkaufsplattformen zu Bewertungszwecken eingerichteten Foren ausgenommen sind, ist wenig überzeugend, weil auch dort ebenso Hass verbreitet werden kann. Zudem wird sich in der Praxis wohl in vielen Fällen nicht eindeutig feststellen lassen, ob ein Diskussionsforum tatsächlich gemäß § 3 Abs 1 SVN-G „auf Nutzer in Österreich ausgerichtet“¹⁰⁴ und deshalb vom Anwendungsbereich des SVN-G umfasst ist. Auch wenn sich die Erläuterungen hier bemühen, diese Anforderung als unproblematisch darzustel-

¹⁰¹ *Al-Youssef*, Regierung will Anonymität im Netz abschaffen – mit hohen Strafen, Website Der Standard 10.04.2019 <www.derstandard.at/story/2000101143621/regierung-will-anonymitaet-im-netz-abschaffen-mit-hohen-strafen> (abgefragt am 14.01.2022);

Brodnig, FPÖ im Internet: Tag für Tag ein Propagandastück, Website Profil 24.05.2016 <www.profil.at/oesterreich/fpoe-strache-internet-tag-tag-propagandastueck-6378335> (abgefragt am 14.01.2022).

¹⁰² Überwachung von Nachrichten und Auskunft über Daten einer Nachrichtenübermittlung nach den Bestimmungen der Strafprozessordnung (StPO), Auskunft über Daten nach den Bestimmungen des Sicherheitspolizeigesetzes (SPG), Auskunft über Daten nach § 11 Abs 1 Z 7 Polizeiliches Staatsschutzgesetz (PStSG), Auskunft über Daten nach § 99 Abs 3a Finanzstrafgesetz (FinStrG) sowie die Erfüllung der Verpflichtungen gemäß § 97 Abs 1a Telekommunikationsgesetz (TKG).

¹⁰³ Verordnung der Bundesministerin für Justiz über den Ersatz der Kosten der Anbieter für die Mitwirkung an der Auskunft über Daten einer Nachrichtenübermittlung, der Auskunft über Vorratsdaten und der Überwachung von Nachrichten (Überwachungskostenverordnung – ÜKVO), BGBl II 322/2004.

¹⁰⁴ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 1.

len,¹⁰⁵ bleibt diese vielseitig interpretierbar, wodurch manche Forenbetreiber zwangsläufig im Ungewissen gelassen werden, ob ihr Dienst den Pflichten des SVN-G unterliegt.

3.7.2 Konflikt mit dem Herkunftslandprinzip

Ein weiteres Problem stellt eine mögliche Verletzung des sogenannten Herkunftslandprinzips dar. Dieses entspringt Art 3 Abs 2 der E-Commerce-Richtlinie,¹⁰⁶ der in der österreichischen Rechtsordnung in § 20 ECG umgesetzt worden ist. Das Herkunftslandprinzip besagt, dass auf Dienste der Informationsgesellschaft grundsätzlich das Recht jenes Mitgliedstaats anzuwenden ist, in dem der Anbieter des Dienstes seine Niederlassung hat.¹⁰⁷ Gemäß Art 3 Abs 4 E-Commerce-RL besteht zwar die Möglichkeit, im nationalen Recht bestimmte Maßnahmen als Ausnahmen vom Herkunftslandprinzip festzulegen, jedoch nur, wenn diese aus einem der angeführten Gründe erforderlich sind, beispielsweise zum „Schutz der öffentlichen Ordnung, Verhütung, Ermittlung, Aufklärung und Verfolgung von Straftaten, [...] der Bekämpfung der Hetze aus Gründen der Rasse, des Geschlechts, des Glaubens oder der Nationalität, sowie von Verletzungen der Menschenwürde einzelner Personen [...]“¹⁰⁸. Das Problem hierbei besteht darin, dass solche Maßnahmen nur jeweils für einen bestimmten Dienst eines konkreten Anbieters ergriffen werden dürfen, jedoch sind allgemeine Maßnahmen für eine ganze Kategorie von Diensten unzulässig.¹⁰⁹ Weil das SVN-G aber sehr wohl eine ganze Kategorie von Diensten, nämlich unterschiedlichste Diskussionsplattformen verschiedener Anbieter betrifft, liegt der Schluss nahe, dass das SVN-G für Plattformbetreiber, die ihre Niederlassung außerhalb von Österreich haben, gar nicht zur Anwendung kommen darf. Damit würden Internetgiganten wie Facebook oder Twitter, die ihren Europasitz oftmals in Irland haben, gar nicht vom SVN-G erfasst sein.

¹⁰⁵ ME SVN-G, 134/ME XXVI. GP Erläut 3.

¹⁰⁶ Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“), ABl L 2000/178, 1.

¹⁰⁷ Zankl, E-Commerce-Gesetz. Kommentar² (2016) § 20 Rz 377.

¹⁰⁸ Art 3 Abs 4 lit a i E-Commerce-RL.

¹⁰⁹ Zankl/Knaipp, Neues IT-Recht, ecolex 2021/73, 106 (106).

Dass im Ergebnis somit zahlreiche Foren, in denen es aber genauso zu Hasskommentaren kommen kann, vom Anwendungsbereich des Entwurfs ausgeklammert werden, teils aufgrund wenig nachvollziehbarer Ausnahmen und Anforderungen des SVN-G, teils wegen der Einschränkungen durch das Herkunftslandprinzip, lässt bereits an dieser Stelle den Eindruck entstehen, dass das SVN-G letztendlich kein geeignetes Mittel darstellen könnte, um dem Problem „Hass im Netz“ wirksam entgegenzutreten zu können.

Trotz aller Kritik ist jedoch zu berücksichtigen, dass der hier gegenständliche Ministerialentwurf des SVN-G nach Abschluss des Begutachtungsverfahrens, und auch aufgrund der Regierungswechsel nach der sogenannten Ibiza-Affäre, bis dato nicht mehr weiterverfolgt worden ist. Es ist also durchaus denkbar, dass vor der Einbringung im Nationalrat noch Korrekturen am Entwurf vorgenommen worden wären, die zumindest einige der dargestellten Probleme behoben oder wenigstens entschärft hätten. Aufgrund der Vielzahl der Unzulänglichkeiten des Entwurfs ist jedoch in Frage zu stellen, ob eine Verbesserung im nötigen Umfang überhaupt möglich gewesen wäre.

4. SVN-G bewirkt anlasslose Vorratsdatenspeicherung

Unterzieht man die mit dem SVN-G auferlegten Datensammelungs- und verarbeitungspflichten nun einer Gesamtbetrachtung, dann stellt man fest, dass die Umsetzung des SVN-G durch die Diensteanbieter eine umfangreiche und systematische Speicherung personenbezogener Daten bewirken würde. Diese Maßnahmen würden anlasslos und unterschiedslos sämtliche Nutzer von umfassten Diskussionsforen einschließen und damit einen sehr großen Personenkreis betreffen, ohne Rücksicht darauf zu nehmen, ob sich die Nutzer tatsächlich etwas zuschulden kommen lassen. Die Speicherung dieser personenbezogenen Daten ist grundsätzlich für den Betrieb von Diskussionsforen in keiner Weise notwendig. Die Speicherpflicht wird den Diensteanbietern allein zu dem Zweck aufgezungen, um die auf Vorrat gesammelten Daten für die Verfolgung möglicher zukünftiger Rechtsverstöße der Forennutzer heranziehen zu können. Dass es tatsächlich zu solchen Verstößen kommen wird, ist dabei jedoch keineswegs absehbar und wird bei der ganz überwiegenden Mehrheit der Nutzer wohl auch nie eintreten.

Dieses Konzept des SVN-G zeigt deutliche Parallelen zur äußerst umstrittenen und viel diskutierten Vorratsdatenspeicherung von Telekommunikationsdaten, die bis zu ihrer Aufhebung durch den Verfassungsgerichtshof (VfGH) im Jahr 2014 in Österreich gesetzlich angeordnet war. Bis einschließlich 30.06.2014 waren die österreichischen Telekomunternehmen verpflichtet, in großem Umfang personenbezogene Daten ihrer Kunden, die bei der Nutzung von Telekommunikationsdiensten anfallen, anlasslos auf Vorrat zu speichern, um später für eventuelle Strafverfolgungszwecke darauf zurückgreifen zu können. Die nationalen Rechtsnormen, die diese Speicherverpflichtung auferlegten, hatten ihren Ursprung in der Vorratsdatenspeicherungsrichtlinie der Europäischen Union vom 15.03.2006.¹¹⁰

Nachdem jedoch der Europäische Gerichtshof im durch ein Ersuchen auf Vorabentscheidung durch den österreichischen VfGH erfolgten Urteil in der verbundenen Rechtssache *Digital Rights Ireland* und *Seitlinger u.a.* vom 08.04.2014¹¹¹ die Vorratsdatenspeicherungsrichtlinie für ungültig erklärt hat, hat in der Folge der VfGH mit seinem

¹¹⁰ Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl L 2006/105, 54.

¹¹¹ EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*).

Erkenntnis G 47/2012 ua vom 27.06.2014¹¹² die zur Umsetzung dieser Richtlinie in Österreich geschaffenen nationalen Rechtsnormen aufgehoben. Seit dem 01.07.2014 ist somit die anlasslose Vorratsdatenspeicherung in der bis dahin angewandten Form in Österreich nicht mehr zulässig.¹¹³ Seitdem dürfen zu Strafverfolgungszwecken nur noch sogenannte Betriebsdaten an die Ermittlungsbehörden herausgegeben werden, also solche Daten, die die Telekomunternehmen selbst für die Erbringung ihrer Dienste betriebsbedingt speichern müssen.¹¹⁴

Der VfGH hat in diesem richtungsweisenden Erkenntnis zur Vorratsdatenspeicherung vom 27.06.2014 auf Basis des EuGH-Urteils *Digital Rights Ireland* im Wesentlichen festgestellt, dass derartige Eingriffsmaßnahmen, die die anlasslose Speicherung personenbezogener Daten eines sehr großen Betroffenenkreises auf Vorrat anordnen, ausschließlich zur Verfolgung schwerer Kriminalität und unter Einhaltung strenger Sicherheitsvorkehrungen erfolgen dürfen sowie einer richterlichen Kontrolle unterliegen müssen.¹¹⁵

Auf europäischer Ebene hat der EuGH in einem weiteren maßgeblichen Urteil vom 21.12.2016 in der verbundenen Rechtsache *Tele2 Sverige* und *Watson u.a.*¹¹⁶ die vorangegangene Entscheidung *Digital Rights Ireland* grundsätzlich bestätigt und schließlich die verbliebenen Freiräume für nationale Bestimmungen zur Speicherung von Daten auf Vorrat zu Strafverfolgungszwecken, die sich aus Art 15 Abs 1 der Datenschutzrichtlinie der Europäischen Union für elektronische Kommunikation (E-Privacy-Richtlinie)¹¹⁷ ergeben, noch deutlicher abgesteckt und klare Voraussetzungen dafür geschaffen.

¹¹² VfGH 27.06.2014, G 47/2012, G 59/2012, G 62/2012, G 70/2012, G 71/2012.

¹¹³ Kundmachung des Bundeskanzlers über die Aufhebung von Bestimmungen des Telekommunikationsgesetzes 2003, der Strafprozeßordnung 1975 und des Sicherheitspolizeigesetzes durch den Verfassungsgerichtshof, BGBl I 44/2014 (kundgemacht am 30.06.2014); Die Presse, Website 01.07.2014, Vorratsdatenspeicherung in Österreich außer Kraft <www.diepresse.com/3830407/vorratsdatenspeicherung-in-osterreich-ausser-kraft> (abgefragt am 14.01.2022).

¹¹⁴ §§ 102a bis 102c TKG 2003 idF BGBl I 78/2018, nicht zu verwechseln mit den am 30.06.2014 außer Kraft getretenen Vorgängerbestimmungen zur aufgehobenen Vorratsdatenspeicherung.

¹¹⁵ VfGH 27.06.2014, G 47/2012 ua, Rz 168 und 171.

¹¹⁶ EuGH 21.12.2016, C-203/15, C-698/15 (*Tele2 Sverige* und *Watson u.a.*).

¹¹⁷ Art 15 Abs 1 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABi L 2002/201, 37 idF ABi L 2009/337, 11.

Diese Rechtsprechung wurde zuletzt in den Jahren 2020 und 2021 durch zwei weitere Urteile des EuGH zur Vorratsdatenspeicherung, EuGH 06.10.2020, C-623/17 (*Privacy International*)¹¹⁸ und EuGH 02.03.2021, C-746/18 (*Prokuratuur*),¹¹⁹ weiter gefestigt,¹²⁰ zudem wird auch in den Schlussanträgen des Generalanwalts vom 18.11.2021 in aktuell noch anhängigen Rechtssachen erneut auf diese hingewiesen.¹²¹

Dass die seit dem Erkenntnis vom 27.06.2014 bestehenden grundlegenden Rechtsprechung des VfGH nicht allein auf die Vorratsdatenspeicherung von Telekommunikationsdaten anzuwenden ist, sondern diese als allgemeiner Maßstab für die anlasslose Vorratsspeicherung von personenbezogenen Daten zu Strafverfolgungszwecken zu verstehen ist, hat der VfGH zuletzt in seinem Erkenntnis zum sogenannten „Sicherheitspaket“¹²² verdeutlicht. Dabei handelte es sich um ein im Jahr 2018 ebenfalls von der damaligen ÖVP-FPÖ-Regierungskoalition initiiertes Gesetzespaket, welches die Datenverarbeitungsbefugnisse der Strafverfolgungsbehörden drastisch erweitern sollte. Auch dieses Gesetzespaket wurde vehement kritisiert und von Gegnern sinnbildlich als „Überwachungspaket“ bezeichnet.¹²³ Neben der Einführung des berüchtigten „Bundestrojaners“, sollten mit den vorgesehenen gesetzlichen Änderungen unter anderem die Sicherheitsbehörden ermächtigt werden, mittels des Einsatzes von bildverarbeitenden technischen Einrichtungen verschiedenste Daten zur Identifizierung von Kraftfahrzeugen, aber auch Daten aller Fahrzeuginsassen anlasslos und noch dazu verdeckt zu ermitteln und für die

¹¹⁸ EuGH 06.10.2020, C-623/17 (*Privacy International*).

¹¹⁹ EuGH 02.03.2021, C-746/18 (*Prokuratuur*).

¹²⁰ Die Urteile EuGH 21.12.2016, C-203/15, C-698/15 (*Tele2 Sverige und Watson u.a.*), EuGH 06.10.2020, C-623/17 (*Privacy International*) und EuGH 02.03.2021, C-746/18 (*Prokuratuur*) behandeln jeweils nationale Rechtsnormen zur Vorratsdatenspeicherung von Telekommunikationsdaten, die die jeweiligen EU-Mitgliedstaaten auf Basis des Art 15 Abs 1 der Datenschutzrichtlinie (E-Privacy-Richtlinie) erlassen hatten.

¹²¹ GA 18.11.2021, C-793/19, C-794/19 (*SpaceNet und Telekom Deutschland*);
GA 18.11.2021, C-14/20 (*Commissioner of the Garda Síochána u.a.*);
GA 18.11.2021, C-339/20, C-397/20 (*VD und SR*).

¹²² Bundesgesetz, mit dem das Sicherheitspolizeigesetz, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden, BGBl I 29/2018;
Bundesgesetz, mit dem die Strafprozeßordnung 1975, das Staatsanwaltschaftsgesetz und das Telekommunikationsgesetz 2003 geändert werden (Strafprozessrechtsänderungsgesetz 2018), BGBl I 27/2018.

¹²³ *Al-Youssef*, Verfassungsgerichtshof hinterfragt Überwachungspaket, Website Der Standard 25.06.2019 <www.derstandard.at/story/2000105396116/bundestrojaner-und-autobahnueberwachung-vor-dem-vfgh> (abgefragt am 14.01.2022).

Verfolgung beliebiger Straftatbestände zu verarbeiten. Zudem hat der Gesetzgeber den Sicherheitsbehörden die Möglichkeit eröffnet, zum selben Zweck auch auf Daten und insbesondere Bilddaten zurückzugreifen, die bei der sogenannten abschnittsbezogenen Geschwindigkeitsüberwachung, gemeinhin besser bekannt als „Section-Control“, gewonnen werden und welche ebenfalls auf Vorrat zu speichern gewesen wären. Die betreffenden Bestimmungen im Sicherheitspolizeigesetz, der Straßenverkehrsordnung und der Strafprozessordnung wurden vom VfGH jedoch als verfassungswidrig aufgehoben, da sie unter anderem maßgeblich gegen die Kriterien der Vorratsdaten-Rechtsprechung des VfGH verstießen.¹²⁴

4.1 Parallelen zur Vorratsdatenspeicherung von Telekommunikationsdaten

Aber nicht nur das Grundkonzept des SVN-G ähnelt stark dem der Vorratsdatenspeicherung von Telekommunikationsdaten, vielmehr finden sich darüber hinaus noch weitere Parallelen zwischen diesen beiden Maßnahmen.

4.1.1 Eingriffe in elektronische Kommunikation

So bewirken sowohl die Vorratsdatenspeicherung von Telekommunikationsdaten als auch die Identifizierungspflicht des SVN-G staatlich erzwungene Eingriffe in Formen von Kommunikation.

Tauschen sich Bürger unter Verwendung von elektronischen Kommunikationsmitteln wie klassischen Telekommunikationsdiensten oder beispielsweise per E-Mail aus, dann liegen Fälle von sogenannter individueller bzw vertraulicher Kommunikation vor.¹²⁵ Die Vertraulichkeit, die sich auf den Inhalt dieser Art von Kommunikation bezieht, unterliegt dabei dem besonderen Grundrechtsschutz des in Art 10a StGG verankerten Fernmeldegeheim-

¹²⁴ VfGH 11.12.2019, G 72-74/2019, G 181-182/2019;

Kundmachung der Bundeskanzlerin über die Aufhebung des § 54 Abs. 4b und des § 57 Abs. 2a des Sicherheitspolizeigesetzes, des § 98a Abs. 2 erster Satz der Straßenverkehrsordnung 1960 und des § 134 Z 3a und des § 135a der Strafprozeßordnung 1975 durch den Verfassungsgerichtshof, BGBl I 113/2019 (kundgemacht am 27.12.2019).

¹²⁵ *Berka*, Öffentliches Recht. Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT I/1 (2012) 74.

nisses, der durch Art 8 EMRK, das Grundrecht auf Achtung des Privat- und Familienlebens, ergänzt wird.¹²⁶

Beim zentralen Anwendungsbereich des SVN-G, also dem Posten von Kommentaren auf Internet-Diskussionsplattformen, handelt es sich ebenso um eine Form von Kommunikation, und zwar im Regelfall um sogenannte öffentliche Kommunikation, die nicht dem Schutz des Fernmeldegeheimnisses untersteht.¹²⁷ Schließlich sind die Kommentare in den meisten Internetforen öffentlich einsehbar, einzige Zugangshürde, um die Postings lesen zu können, ist oft lediglich eine Registrierung mit einer E-Mail-Adresse, die aber theoretisch jedermann offen steht. Öffentliche Kommunikation im Internet unterliegt dem grundrechtlichen Schutz von Art 10 EMRK.¹²⁸ Anders verhält sich dies aber in sogenannten geschlossenen Foren, in denen nur ausgewählten Nutzern eine Zugangsberechtigung gewährt wird und die Kommentare daher nicht öffentlich einsehbar sind.¹²⁹ Die Kommunikation in solchen geschlossenen Foren fällt wiederum sehr wohl in den Schutzbereich des Art 10a StGG, da es sich hierbei um eine Form von vertraulicher Kommunikation handelt.¹³⁰

Auf den ersten Blick scheint es, dass die Meinungsäußerung in offenen Diskussionsforen keinem Geheimhaltungsinteresse unterliegen würde, da solche Foren schließlich öffentlich einsehbar sind, und die Nutzer es deshalb in Kauf nehmen würden, dass ihre Kommentare theoretisch jedermann zugänglich werden könnten. Demnach wäre aufgrund mangelnder Vertraulichkeit die Kommunikation in Diskussionsforen deutlich weniger schutzwürdig als beispielsweise klassische Telekommunikation.

Dem ist jedoch entgegenzuhalten, dass Verfasser von Kommentaren in Internetforen es zwar billigen oder sogar beabsichtigen, ihre Meinungen und Ansichten einer mehr oder weniger breiten Öffentlichkeit zugänglich zu machen, dabei jedoch zumeist nicht

¹²⁶ VfGH 29.06.2012, B 1031/11 VfSlg 19.657/2012;

Hengstschläger/Leeb, Grundrechte³ (2019) 224;

Berka, Öffentliches Recht. Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT I/1 (2012) 74 ff;

Berka/Trappel, Internetfreiheit in Österreich, REM Bd 17 (2019) 5.

¹²⁷ VfGH 29.06.2012, B 1031/11 VfSlg 19.657/2012;

Hengstschläger/Leeb, Grundrechte³ (2019) 224.

¹²⁸ *Berka/Trappel*, Internetfreiheit in Österreich, REM Bd 17 (2019) 4;

Berka, Öffentliches Recht. Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT I/1 (2012) 77 ff.

¹²⁹ VfGH 29.06.2012, B 1031/11 VfSlg 19.657/2012.

¹³⁰ *Hengstschläger/Leeb*, Grundrechte³ (2019) 224.

wünschen, dass ihre Identität bekannt wird. Beim Diskurs in Internetforen steht also typischerweise die Meinung selbst im Vordergrund, während die Identität der Person, die diese Meinung vertritt, in der Regel keine Rolle spielt. Durch die in solchen Foren übliche Verwendung eines Pseudonyms anstatt des bürgerlichen Namens, haben die Nutzer die Möglichkeit, ihre Identität zu schützen. So betrachtet, kommt den Nutzern bei der Kommunikation in Internetforen sehr wohl ein Geheimhaltungsinteresse im Sinne einer Vertraulichkeit zu, zwar nicht bezüglich des Inhalts der Kommunikation, sondern betreffend ihre Identität.

Ein Identifizierungszwang, wie ihn das SVN-G vorsieht, steht diesem Geheimhaltungsinteresse jedoch entgegen, da dieser die bisher in Internetforen weitgehend gewohnte Möglichkeit zur vollkommen anonymen Meinungsäußerung beseitigen würde.

4.1.2 Ähnlichkeit der betroffenen Datenkategorien

Darüber hinaus weisen auch die Kategorien von personenbezogenen Daten, die im Rahmen der Identifizierungspflicht des SVN-G in Diskussionsforen gespeichert und verarbeitet werden müssten und jenen Daten, die bei der Vorratsdatenspeicherung von Telekommunikationsdaten betroffen waren, deutliche Übereinstimmungen auf. Die Registrierungsdaten, also Name und Adresse der Forennutzer, ebenso wie das von den Nutzern gewählte Pseudonym entsprechen den Stammdaten im Sinne des § 92 Abs 3 Z 3 Telekommunikationsgesetz 2003 (TKG).¹³¹ Die Adressen der Nutzer können zudem auch mit Standortdaten¹³² im Sinne des § 92 Abs 3 Z 6 TKG verglichen werden. Die Inhalte von Postings kommen den Inhaltsdaten¹³³ im Sinne des § 92 Abs 3 Z 5 TKG gleich, also dem Gesprächsinhalt von Telefongesprächen oder dem Inhalt von Textnachrichten. Die Zeitstempel, die die Einloggzeiten der Forennutzer aufzeichnen, kann man in etwa mit Verkehrsdaten¹³⁴ im Sinne des § 92 Abs 3 Z 4 TKG bzw Zugangsdaten¹³⁵ im Sinne des § 92 Abs 3 Z 4a TKG vergleichen, also mit Daten, die neben vielen anderen Informationen unter anderem auch Zeit und Dauer von geführten Telefongesprächen ausweisen.

¹³¹ Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 – TKG 2003), BGBl I 70/2003 idF I 148/2021.

¹³² § 92 Abs 3 Z 6 TKG.

¹³³ § 92 Abs 3 Z 5 TKG.

¹³⁴ § 92 Abs 3 Z 4 TKG.

¹³⁵ § 92 Abs 3 Z 4a TKG.

4.2 Unterschiede zur Vorratsdatenspeicherung von Telekommunikationsdaten

Neben den angeführten Überschneidungen liegt jedoch auch ein wesentlicher Unterschied vor, der darin besteht, dass die bei der Vorratsspeicherung von Telekommunikationsdaten zu sammelnden Daten beim Betrieb von Telekommunikationsdiensten ohnehin anfielen. Auch die Stammdaten der Kunden, also Name und Adresse, mussten von den Telekom-anbietern ohnedies gespeichert werden, weil diese für Vertragserfüllung und Verrechnungszwecke notwendig waren. Der entscheidende Eingriff war die vom Gesetzgeber auferlegte Pflicht, diese Daten für einen bestimmten Zeitraum über den betriebsnotwendigen Zeitraum hinaus gespeichert zu behalten.

Grundlegend anders ist die Situation im Anwendungsbereich von Identifizierungspflichten wie dem SVN-G. Die Daten, die aufgrund des SVN-G gespeichert werden müssen, werden für den Betrieb eines Onlineforums grundsätzlich gar nicht benötigt. Der Diensteanbieter hat in der Regel selbst kein Interesse, die Identität und Wohnadresse der Forennutzer zu kennen. Die Verarbeitung und Speicherung dieser Daten ist also nicht betriebsnotwendig, sondern wird erst durch das SVN-G erzwungen. In dieser Hinsicht bedeutet die Verpflichtung diese Daten zu sammeln und zu speichern somit eine stärkere Belastung für die Diensteanbieter, als es bei der Vorratsdatenspeicherung von Telekommunikationsdaten der Fall war, da dort Stammdaten, Verkehrsdaten und Standortdaten ohnehin betriebsbedingt bzw zur Erfüllung der Kundenverträge verarbeitet werden mussten.

Ein weiterer entscheidender Unterschied liegt in der Betroffenheit von Kommunikationsinhalten. Die Inhalte der Kommunikation waren von der Speicherverpflichtung der Vorratsdatenspeicherung von Telekommunikationsdaten nämlich ausgenommen. Die Telekom-anbieter mussten die Inhalte der Telefongespräche und Nachrichten ihrer Kunden also nicht aufzeichnen. Das SVN-G hingegen ordnet explizit an, dass die Diensteanbieter auch Aufzeichnungen von Postinginhalten anfertigen und an die um Übermittlung ansuchenden Stellen herausgeben müssen.¹³⁶ Damit sind durch die Maßnahmen des SVN-G mit den Postinginhalten auch Kommunikationsinhalte betroffen. Diese sind zwar in den meisten Foren ohnehin öffentlich zugänglich, jedoch ist dabei die Identität der Verfasser durch die

¹³⁶ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 4 Abs 4.

Anonymität geschützt. Die Anonymität würde aber durch die Einführung der Identifizierungspflicht des SVN-G beseitigt werden.

Die soeben veranschaulichten starken Parallelen der durch den Identifizierungszwang veranlassten Datensammlungspflicht des SVN-G zur Vorratsdatenspeicherung von Telekommunikationsdaten verdeutlichen, dass sich die Maßnahmen des SVN-G in vielerlei Hinsicht im Kontext der richtungsweisenden Entscheidungen und Grundsätze des VfGH und des EuGH zur Vorratsdatenspeicherung personenbezogener Daten zu Strafverfolgungszwecken betrachten lassen. Deshalb dient diese grundlegende höchstgerichtliche Rechtsprechung auch als Maßstab für die folgende Grundrechtsprüfung der Maßnahmen des SVN-G.

5. Grundrechtsprüfung

Es ist offensichtlich, dass die im SVN-G angeordneten Maßnahmen verschiedene Grundrechte der Rechtsunterworfenen berühren. Im Folgenden soll das Hauptaugenmerk auf die Prüfung möglicher Eingriffe in Grundrechte der Nutzer der Diskussionsforen gelegt werden. Auch wenn die eigentlichen Normadressaten des SVN-G die Diensteanbieter sind, so sind es in erster Linie die Nutzer, deren Grundrechte tangiert werden und die damit die Auswirkungen der Identifizierungspflicht des SVN-G zu spüren bekommen. Vorrangiges Ziel des Gesetzesentwurfs ist es schließlich, das „Wohlverhalten“ der Forennutzer zu sichern und nicht jenes der Diensteanbieter. Auf etwaige Einschränkungen von verfassungsgesetzlich gewährleisteten Rechten der Diensteanbieter wird daher im Folgenden nicht näher eingegangen.¹³⁷

Die Prüfung von nationalen Gesetzen auf ihre Verfassungskonformität und das Vorliegen von Grundrechtsverletzungen obliegt dem Verfassungsgerichtshof. Als Prüfungsmaßstab würde der VfGH üblicherweise die in der EMRK bzw der übrigen nationalen Rechtsordnung verankerten Grundrechte heranziehen und nicht die in der Grundrechtecharta der Europäischen Union (GRC)¹³⁸ garantierten Rechte.

Die zu prüfenden grundlegenden Maßnahmen des SVN-G sind die Speicherung, Verarbeitung und Übermittlung von personenbezogenen Daten der Nutzer der betroffenen Diskussionsforen. Durch diese Datenverarbeitungsmaßnahmen werden verschiedene verfassungsgesetzlich gewährleistete Rechte der Nutzer berührt, in erster Linie betreffen diese unweigerlich deren Grundrecht auf Datenschutz (§ 1 DSG). Damit einher geht eine mögliche Einschränkung des Grundrechts der Forennutzer auf Achtung des Privat- und Familienlebens (Art 8 EMRK), weil die Speicherung und Verwendung personenbezogener Daten einen Eingriff in die grundrechtlich geschützte Privatsphäre, insbesondere den von Art 8 EMRK ebenfalls gewährleisteten Schutz persönlicher Daten darstellt.¹³⁹ Da Diskus-

¹³⁷ Bei den Diensteanbietern wären in erster Linie Eingriffe in das Grundrecht auf Erwerbsfreiheit (Art 6 Abs 1 StGG) zu erwarten, verursacht durch die Vorschriften des SVN-G, die die Diensteanbieter verpflichten, die geforderten Datenverarbeitungsmaßnahmen in ihren Onlinediensten umzusetzen.

¹³⁸ Charta der Grundrechte der Europäischen Union, ABl C 2007/303, 1; ABl C 2010/83, 389; ABl C 2012/326, 391; ABl C 2016/202, 389; BGBl III 132/2009.

¹³⁹ *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention⁷ (2021) 299 Rz 10 und 311 Rz 27.

sionsforen der Kommunikation und dem Meinungsaustausch der Nutzer dienen, ist zudem ein Eingriff in das Grundrecht auf Freiheit der Meinungsäußerung (Art 10 EMRK) zu prüfen.

5.1 Prüfungsmaßstab der Grundrechtsprüfung

Da es sich, wie bereits dargestellt, beim SVN-G ebenfalls in erster Line um ein Werkzeug zur Strafverfolgung mittels anlasslos und systematisch auf Vorrat gespeicherter personenbezogener Daten handelt, von dem sämtliche Nutzer von Onlineforen unterschiedslos betroffen sind und damit letztendlich ganz überwiegend Bürger, die bei der Nutzung dieser Diskussionsplattformen zu keiner Zeit einen Anlass für Strafverfolgungsmaßnahmen begründen, wird auf die Prüfung des SVN-G die für derartige Fälle maßgebliche, grundlegende Rechtsprechung des österreichischen Verfassungsgerichtshofs zur Vorratsdatenspeicherung, die unter anderem auch auf den Entscheidungen des Europäischen Gerichtshofs *Digital Rights Ireland* und *Tele2 Sverige* basiert, angewendet.

Weil in den Entscheidungen des VfGH und des EuGH zur Vorratsdatenspeicherung Feststellungen und rechtliche Beurteilungen zu zahlreichen konkreten Sachverhalten und Fragestellungen getroffen wurden, die sich in sehr ähnlicher Form auch bei der Prüfung des SVN-G wiederfinden, und zudem in beiden Fällen exakt dieselben Grundrechte betroffen sind, wird die Grundrechtsprüfung hinsichtlich der Maßnahmen des SVN-G im Folgenden basierend auf einer Zusammenschau dieser vorangegangenen höchstgerichtlichen Entscheidungen vorgenommen.¹⁴⁰ Auch das Erkenntnis des VfGH zum „Sicherheitspaket“ wird dabei herangezogen, da darin ebenfalls ein vergleichbarer Fall von anlassloser Vorratsdatenspeicherung behandelt wurde und dieses ebenso Feststellungen und Beurteilungen zu konkreten Problemstellungen enthält, die annähernd identisch auch beim SVN-G vorkommen. Liegen zu einzelnen Fragen der folgenden Grundrechtsprüfung des SVN-G bereits Beurteilungen der Höchstgerichte in den genannten Vorratsdaten-

¹⁴⁰ Hier ist darauf hinzuweisen, dass der EuGH die in den Urteilen *Digital Rights Ireland* und *Tele2 Sverige* gegenständliche Prüfung am Maßstab der Charta der Grundrechte der Europäischen Union (GRC) durchgeführt hat. Hingegen würde der VfGH, wie bereits im grundlegenden Erkenntnis VfGH 27.06.2014, G 47/2012 ua, die Prüfung des SVN-G üblicherweise nach der EMRK und dem DSG durchführen. Dennoch können die konkreten Beurteilungen des EuGH aufgrund der weitgehenden Inhaltsgleichheit der relevanten Grundrechte in GRC und EMRK bzw DSG für die hier gegenständliche Prüfung nach der EMRK und dem DSG herangezogen werden.

Entscheidungen vor, so soll darauf zurückgegriffen und diese, soweit dies möglich ist, der Bewertung der entsprechenden Fragestellung des SVN-G zugrunde gelegt werden.

5.2 VfGH-Rechtsprechung betreffend anlasslose Vorratsdatenspeicherung

Die im Erkenntnis zur Vorratsdatenspeicherung vom 27.04.2014 getroffene grundlegende Rechtsprechung des VfGH für die Verwendung von Vorratsdaten zur Verfolgung von Straftaten hat dieser zuletzt im Jahr 2019 im Erkenntnis zum „Sicherheitspaket“ neuerlich bekräftigt. Diese besagt, dass Regelungen, die die anlasslose Speicherung von Daten auf Vorrat vorsehen und dabei einen maßgeblichen Grundrechtseingriff darstellen, nur dann verhältnismäßig und daher zulässig sein können, wenn sie der Bekämpfung schwerer Kriminalität dienen, „sofern sie mit den strengen Anforderungen des § 1 DSG und Art. 8 EMRK im Einklang stehen. Ob ein solcher Eingriff im Hinblick auf § 1 Abs. 2 DSG und Art. 8 Abs. 2 EMRK zulässig ist, hängt von der Ausgestaltung der Bedingungen der Speicherung von Daten ‚auf Vorrat‘ und den Anforderungen an deren Löschung sowie von den gesetzlichen Sicherungen bei der Ausgestaltung der Möglichkeiten des Zugriffes auf diese Daten ab“¹⁴¹. Diese grundlegende Rechtsprechung des VfGH stellt den konkreten Maßstab für die folgende Prüfung der Eingriffsmaßnahmen des SVN-G dar.

5.3 Liegen Eingriffe in die genannten Grundrechte vor?

Zu Beginn der Prüfung gilt es festzustellen, ob durch die Maßnahmen des SVN-G tatsächlich Eingriffe in die erwähnten verfassungsgesetzlich gewährleistete Rechte der betroffenen Forennutzer, also das Grundrecht auf Datenschutz (§ 1 DSG), das Grundrecht auf Achtung des Privat- und Familienlebens (Art 8 EMRK) und das Grundrecht auf Freiheit der Meinungsäußerung (Art 10 EMRK), bewirkt werden.

Um das SVN-G auf das Vorliegen eines Eingriffs in das Grundrecht auf Datenschutz und eine damit verbundene Einschränkung des Grundrechts auf Achtung des Privat- und Familienlebens zu prüfen, müssen die im Gesetzesentwurf vorgesehenen Datenverarbeitungs-

¹⁴¹ VfGH 11.12.2019, G 72-74/2019, G 181-182/2019, Rz 100.

maßnahmen genauer betrachtet werden. Zu den Daten, die im Rahmen des SVN-G gespeichert, verarbeitet und übermittelt werden müssen, gehören Vorname, Nachname und die Adresse eines jeden Nutzers, der gewählte Nutzernamen, also das Pseudonym, sowie die verfassten Postings inklusive deren Inhalt. Zudem muss mit den Zeitstempeln, welche die Einloggzeitpunkte der Nutzer und die Nutzungsdauer aufzeichnen, eine weitere mit einem bestimmten Nutzer verknüpfte Datenkategorie verarbeitet werden, die zwar im Text des SVN-G nicht explizit angeführt, aber zur gesetzeskonformen Umsetzung des SVN-G technisch bedingt notwendig ist. Bei all diesen Nutzerdaten, deren Verarbeitung in erster Linie für Zwecke der Ermittlung und Verfolgung von Straftaten gemäß § 36 DSG erfolgt,¹⁴² handelt es sich um personenbezogene Daten im Sinne des § 1 Abs 1 iVm § 36 Abs 2 Z 1 DSG, die das Privat- und Familienleben einer bestimmten Person betreffen und insbesondere durch die Verknüpfung der Daten zudem zahlreiche Rückschlüsse auf deren persönliche Ansichten zulassen und daher einem schutzwürdigen Geheimhaltungsinteresse im Sinne des § 1 Abs 1 DSG unterliegen.¹⁴³

Die im SVN-G vorgeschriebene Verarbeitung dieser Daten, die als ersten Schritt die Speicherung durch den Diensteanbieter vorsieht, stellt einen Eingriff in das Grundrecht auf Datenschutz (§ 1 DSG) und damit verbunden unweigerlich auch einen Eingriff in das Grundrecht auf Achtung des Privat- und Familienlebens (Art 8 EMRK) dar.¹⁴⁴

Die weiteren Verarbeitungsschritte, nämlich der Zugriff auf die gespeicherten Daten durch den Diensteanbieter, den dieser vornehmen muss, wenn ihm vermeintlich rechtswidrige Postings gemeldet werden, die Begutachtung und Auswertung des Inhalts dieser Postings und schließlich die Übermittlung der personenbezogenen Daten eines bestimmten Nutzers an Gerichte, Behörden oder Dritte, sowie die Weiterverarbeitung durch diese, bedeuten jeweils weitere Eingriffe in § 1 DSG und Art 8 EMRK.¹⁴⁵ Dass diese Datenverarbeitungsschritte durch die Diensteanbieter vorgenommen werden, also durch in der Regel privatrechtliche Unternehmen, ändert natürlich nichts daran, dass der Grundrechtseingriff

¹⁴² § 36 DSG.

¹⁴³ Vgl VfGH 27.06.2014, G 47/2012 ua, Rz 159.

¹⁴⁴ Vgl VfGH 27.06.2014, G 47/2012 ua, Rz 163;

vgl EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland und Seitlinger u.a.*) Rz 34.

¹⁴⁵ Vgl EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland und Seitlinger u.a.*) Rz 35; vgl VfGH 27.06.2014, G 47/2012 ua, Rz 163.

dem Gesetzgeber zuzurechnen ist, der schließlich die Diensteanbieter gesetzlich zur Durchführung der Maßnahmen verpflichtet.¹⁴⁶

Das in Art 10 EMRK verankerte Grundrecht der Freiheit der Meinungsäußerung ist von besonders hohem Stellenwert, da es einen entscheidenden Fundamentstein einer jeden modernen Demokratie bildet.¹⁴⁷ Die vom SVN-G erfassten Diskussionsplattformen bieten den Nutzern eine wesentliche Möglichkeit, von diesem Grundrecht Gebrauch zu machen und auf unkomplizierte Weise mit anderen Menschen in Interaktion zu treten. Solche Foren erlauben es, ein nahezu uneingeschränktes Publikum zu erreichen, da sie typischerweise weltweit für jede Person, die Zugang zum freien Internet hat, abrufbar sind.

Da der Staat nunmehr mit der Identifizierungspflicht des SVN-G vorgeben will, unter welchen Bedingungen die Bürger Zugang zu den betroffenen Diskussionsplattformen bekommen dürfen, wird das Recht auf freie Meinungsäußerung eingeschränkt. Denn „nach jüngeren Judikaten des VfGH [kommt - *Anm. d. Verf.*] ein Eingriff in die Meinungsfreiheit nicht nur bei intentionalen Beschränkungen des Schutzbereichs, sondern schon dann in Betracht, wenn ein Akt [, wie die einzelnen Maßnahmen des SVN-G, - *Anm. d. Verf.*] die Meinungsfreiheit nur in seinen Auswirkungen behindert.“¹⁴⁸

Darüber hinaus wird die bis dahin gegebene Anonymität der Meinungsäußerung durch den Zwang zur namentlichen Registrierung der Nutzer in den betroffenen Foren gewissermaßen beseitigt. In Summe bedeutet dies eine Form von staatlicher Kontrolle des Kommunikationsverhaltens der Bürger, was einen Eingriff in Art 10 EMRK darstellt.¹⁴⁹

5.4 Exkurs: Verletzung des Wesensgehalts der betroffenen Grundrechte?

Da der EuGH im Urteil *Digital Rights Ireland* die Vorratsdatenspeicherungsrichtlinie am Maßstab der Grundrechtecharta der Europäischen Union bewertet hat, hat er entsprechend

¹⁴⁶ Vgl VfGH 27.06.2014, G 47/2012 ua, Rz 161.

¹⁴⁷ Hengstschläger/Leeb, Grundrechte³ (2019) 242.

¹⁴⁸ Hengstschläger/Leeb, Grundrechte³ (2019) 247; siehe dazu auch *Bezemek*, Freie Meinungsäußerung. Fragen des Grundrechtseingriffs, Fragen der Grundrechtsausübung, ZÖR 2012, 557 (560 ff).

¹⁴⁹ Vgl *Berka*, Öffentliches Recht. Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT I/1 (2012) 78.

Art 52 Abs 1 GRC auch die Prüfung hinsichtlich möglicher Verletzungen des sogenannten Wesensgehalts der betroffenen Grundrechte vorgenommen. Diese Prüfungsschritte kommen zwar in der Grundrechtsprüfung des VfGH nicht immer bzw nicht bei allen Grundrechten in dieser Form vor, bieten aber dennoch weitere Sichtweisen, die auch auf die Beurteilung des SVN-G am Maßstab der EMRK übertragen werden können, weshalb im folgenden kurzen Exkurs darauf eingegangen werden soll. Art 52 Abs 1 GRC sieht vor, dass gesetzlich auferlegte Einschränkungen von in der Charta anerkannten Grundrechten nicht den Wesensgehalt dieser Grundrechte verletzen dürfen. Der EuGH sieht den Wesensgehalt als den unverletzbaren Kerngehalt eines Grundrechts, und prüft in konkreten Fällen als zusätzliche Entscheidung, ob dieser verletzt ist.¹⁵⁰

Die im Anwendungsbereich des SVN-G vorgesehenen Eingriffe in das Recht auf Achtung des Privat- und Familienlebens führt dazu, dass hier eine umfangreiche Datensammlung, die Rückschlüsse auf die Gedankenwelt und die persönlichen Ansichten der betroffenen Nutzer ermöglicht, angelegt werden muss. Anders als die für ungültig erklärte Vorratsdatenspeicherungsrichtlinie sieht das SVN-G nämlich auch eine zumindest bedingte Speicherverpflichtung für Kommunikationsinhalte, also die Postings, vor. Des Weiteren sind die Diensteanbieter praktisch dazu verpflichtet, den Inhalt bestimmter Postings zu analysieren, damit sie beurteilen können, ob ein Ansuchen einer berechtigten Stelle auf Herausgabe zulässig ist.

Der EuGH erachtete bei der Prüfung der Vorratsdatenspeicherungsrichtlinie die Kenntnisnahme vom Inhalt einer Kommunikation als das entscheidende Kriterium für die Beurteilung, ob ein Verletzung des Wesensgehalts des Grundrechts auf Achtung des Privat- und Familienlebens vorliegt.¹⁵¹ Daher könnte man im Fall des SVN-G, zumindest betreffend die Pflicht zur Anfertigung und Herausgabe von Aufzeichnungen von Kommentaren, annehmen, dass bereits der Wesensgehalt des Grundrechts auf Achtung des Privat- und Familienlebens verletzt sein könnte, weil der Eingriff eben auch die Kenntnisnahme des Inhalts der Postings einschließt. Dies folgt aus einem Umkehrschluss der im Urteil *Digital Rights Ireland* vom EuGH getroffenen Bewertung, dass das Nichtgestatten der Kenntnisnahme des Inhalts der Kommunikation bei einer Speicherverpflichtung auf Vorrat dazu

¹⁵⁰ Rumler-Korinek/Vranes in Holoubek/Lienbacher (Hrsg), Charta der Grundrechte der Europäischen Union. GRC-Kommentar² (2019) Art 52 Rz 18.

¹⁵¹ EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 39.

führt, dass der Wesensgehalt des Grundrechts auf Achtung des Privat- und Familienlebens nicht verletzt ist.¹⁵² Gegen eine Verletzung des Wesensgehalts spricht jedoch, dass die Speicherung von an sich öffentlichen Postings keinesfalls so schwer wiegt wie die Speicherung und damit Kenntnisnahme von vertraulicher Kommunikation.

Worin der Wesensgehalt des Grundrechts auf Schutz personenbezogener Daten (Art 8 GRC) genau liegt, hat der EuGH bisher nicht bestimmt.¹⁵³ Jedenfalls sind Eingriffe, die einer Aufhebung des Grundrechts gleichkommen, definitiv unzulässig.¹⁵⁴ Entsprechend der im Urteil des EuGH *Digital Rights Ireland* zur Vorratsdatenspeicherungsrichtlinie getroffenen Feststellung, ist auch im Fall des SVN-G eher davon auszugehen, dass der Wesensgehalt des Grundrechts auf Schutz personenbezogener Daten nicht verletzt ist, weil der Ministerialentwurf immerhin einige wenige auf Datenschutz und Datensicherheit abzielende Regelungen enthält.¹⁵⁵ Diese Datenschutzbestimmungen, wie beispielsweise die erläuterten Löschpflichten betreffend die Registrierungsprofile der Forennutzer, sind jedoch auf den ersten Blick eher knapp geraten. Offensichtlich sind die Verfasser des Entwurfs aber dennoch der Ansicht, dass die im SVN-G enthaltenen Datenverarbeitungsvorgänge hinreichend determiniert sind, um angemessen Schutz und Sicherheit für die Nutzerdaten zu gewährleisten. In den Erläuterungen zum Entwurf wird hierzu noch eher beiläufig angemerkt, dass „weitere davon auszugehen [ist - *Anm. d. Verf.*], dass die Diensteanbieter ihrerseits den Vorgaben der DSGVO oder vergleichbarer Normen unterliegen.“¹⁵⁶ Scheinbar erwarten die Verfasser des Entwurfs, dass am Ende die betroffenen Diensteanbieter selbst sich darum kümmern würden, eventuelle Datenschutzlücken des SVN-G auszugleichen.

¹⁵² Vgl. EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 39; Pavlidis in Holoubek/Lienbacher (Hrsg.), Charta der Grundrechte der Europäischen Union. GRC-Kommentar² (2019) Art 7 Rz 53.

¹⁵³ Riesz in Holoubek/Lienbacher (Hrsg.), Charta der Grundrechte der Europäischen Union. GRC-Kommentar² (2019) Art 8 Rz 96.

¹⁵⁴ Riesz in Holoubek/Lienbacher (Hrsg.), Charta der Grundrechte der Europäischen Union. GRC-Kommentar² (2019) Art 8 Rz 96; Öhlinger/Eberhard, Verfassungsrecht¹² (2019) Rz 713.

¹⁵⁵ Vgl. EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 40.

¹⁵⁶ ME SVN-G, 134/ME XXVI. GP Erläut 5.

Eine Prüfung auf eine mögliche Verletzung des Grundrechts auf Freiheit der Meinungsäußerung (Art 11 GRC) und damit auch auf eine mögliche Verletzung des Wesensgehalts dieses Grundrechts hat der EuGH im Urteil Digital Rights Ireland schließlich nicht mehr vorgenommen. Wie die Erläuterungen zur Charta der Grundrechte klarstellen, liegt eine materielle Kongruenz mit Art 10 EMRK vor, die bewirkt, dass Art 52 Abs 3 GRC zufolge, hierbei die in Art 10 Abs 2 EMRK enthaltenen zulässigen Schranken für Eingriffe in dieses Grundrecht zur Anwendung kommen.¹⁵⁷

5.5 Verhältnismäßigkeitsprüfung

Gemäß der Rechtsprechung des EuGH sind Eingriffsmaßnahmen in Grundrechte nur dann verhältnismäßig, wenn sie „geeignet sind, die mit der fraglichen Regelung zulässigerweise verfolgten Ziele zu erreichen, und nicht die Grenzen dessen überschreiten, was zur Erreichung dieser Ziele geeignet und erforderlich ist“¹⁵⁸, oder mit den Worten des VfGH ausgedrückt, wenn „die Schwere des konkreten Eingriffs nicht das Gewicht und die Bedeutung der mit [dem zu prüfenden Gesetz, also hier dem SVN-G, - *Anm. d. Verf.*] [...] verfolgten Ziele übersteigt.“¹⁵⁹

Eingriffe staatlicher Behörden in das Grundrecht auf Datenschutz und das Grundrecht auf Achtung des Privat- und Familienlebens sind einer strengen Verhältnismäßigkeitsprüfung zu unterziehen und bedürfen einer gesetzlichen Grundlage. Das die Eingriffe ermöglichende Gesetz muss dabei aus einem der in Art 8 Abs 2 EMRK angeführten Gründe auch tatsächlich notwendig sein.¹⁶⁰ Gesetze, die derartige Eingriffe enthalten, dürfen gemäß § 1 Abs 2 zweiter Satz DSG „die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der

¹⁵⁷ Artikel 11 Erläuterungen zur Charta der Grundrechte (2007/C 303/02), ABl C 2007/303, 17; *Bezemek* in Holoubek/Lienbacher (Hrsg), Charta der Grundrechte der Europäischen Union. GRC-Kommentar² (2019) Art 11 Rz 15.

¹⁵⁸ EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 46.

¹⁵⁹ VfGH 27.06.2014, G 47/2012 ua, Rz 166.

¹⁶⁰ *Hengstschläger/Leeb*, Grundrechte³ (2019) 204; *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention⁷ (2021) 318 Rz 37 ff.

Betroffenen festlegen“¹⁶¹. Sollen solche Gesetze die Ermittlung und Verwendung der personenbezogenen Daten für staatliche Verwaltungszwecke eröffnen, muss darin präzise, hinreichend bestimmt und für jedermann vorhersehbar geregelt werden, unter welchen konkreten Voraussetzungen dies erlaubt sein soll.¹⁶² Dies ist vor allem dann zu beachten, wenn es sich um staatliche Überwachungsmaßnahmen handelt, insbesondere wenn diese im Geheimen stattfinden, also ohne Kenntnis des Betroffenen.¹⁶³ Gemäß § 1 Abs 2 letzter Satz DSG darf auch „im Falle zulässiger Beschränkungen [...] der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.“¹⁶⁴ Das bedeutet, dass der Gesetzgeber die spezifische gesetzliche Grundlage derart ausgestalten muss, dass dadurch zulässige Eingriffe in das Grundrecht auf Datenschutz auf das notwendige Mindestmaß begrenzt werden.¹⁶⁵

Staatliche Eingriffe in das Grundrecht auf freie Meinungsäußerung (Art 10 EMRK) sind nur dann verhältnismäßig, wenn sie einem oder mehreren der in Art 10 Abs 2 EMRK angeführten Rechtfertigungsgründe dienen und in einer demokratischen Gesellschaft auch tatsächlich notwendig sind, um diese rechtfertigenden Zwecke zu erreichen.¹⁶⁶

5.5.1 Liegen die Ziele des SVN-G im öffentlichen Interesse?

Das primäre Ziel des SVN-G ist es, die Verfolgung von Straftaten und zivilrechtlichen Ansprüchen zu erleichtern.¹⁶⁷ Das ebenfalls angedachte Ziel der „Förderung des respektvollen Umgangs der Nutzer miteinander“¹⁶⁸ ist jedoch etwas schwerer greifbar. Vermutlich ist damit gemeint, dass das SVN-G auch bezwecken soll, dass Hasspostings von vornherein ganz unterlassen werden. Die Erleichterung der Verfolgung sämtlicher oder einzelner bestimmter Straftaten, wie es das SVN-G je nach Fall vorsieht, würde sich wohl zweifellos

¹⁶¹ § 1 Abs 2 zweiter Satz DSG;

Vgl VfGH 27.06.2014, G 47/2012 ua, Rz 157.

¹⁶² Vgl VfGH 27.06.2014, G 47/2012 ua, Rz 199;

Jahnel, Handbuch Datenschutzrecht (2010) Rz 2/61;

Hengstschläger/Leeb, Grundrechte³ (2019) 205 f.

¹⁶³ *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention⁷ (2021) 318 Rz 39 ff.

¹⁶⁴ § 1 Abs 2 letzter Satz DSG.

¹⁶⁵ Vgl VfGH 27.06.2014, G 47/2012 ua, Rz 158.

¹⁶⁶ *Hengstschläger/Leeb*, Grundrechte³ (2019) 249.

¹⁶⁷ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 1.

¹⁶⁸ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 1.

positiv auf die öffentliche Sicherheit und die öffentliche Ruhe und Ordnung auswirken. Auch die verbesserte Durchsetzbarkeit von zivilrechtlichen Rechtsansprüchen stellt ein achtbares Ziel dar, nämlich den Schutz der „Rechte anderer“¹⁶⁹. Diese Bestrebungen des SVN-G würden dem Gemeinwohl dienen und einer demokratischen Gesellschaft zuträglich sein und damit den Anforderungen der Art 8 Abs 2 und Art 10 Abs 2 EMRK entsprechende Ziele darstellen.¹⁷⁰

5.5.2 Eignung der Maßnahmen zur Erreichung der Ziele

Bei der Prüfung der Eignung der im SVN-G vorgesehenen Verarbeitungsschritte der Nutzerdaten für die Verwirklichung des Ziels der Erleichterung der Verfolgung von Straftaten und Rechtsansprüchen ist davon auszugehen, dass die vorsorgliche Speicherung von Name und Adresse sämtlicher Nutzer die spätere Ermittlung der Urheber von Hasspostings erleichtert und beschleunigt. Die Möglichkeit, auf diese auf Vorrat gespeicherten Daten zurückzugreifen, stellt zumindest eine Vereinfachung für die Strafverfolgungsbehörden dar, Delikte zu verfolgen, und erleichtert es auch Dritten im Sinne des SVN-G, also Privatpersonen und Unternehmen, ihre Rechtsansprüche durchzusetzen.¹⁷¹ Die sofortige Ermittlung des tatsächlichen Verfassers eines Postings wird damit aber dennoch nicht in allen Fällen zu gewährleisten sein, wenn man beispielsweise die Möglichkeit bedenkt, dass stets auch eine andere Person, unter eventuell auch unerlaubter Verwendung der Zugangsdaten eines registrierten Nutzers, ein Posting verfasst haben könnte. Das im Entwurf des SVN-G ausgegebene Ziel, die Verfolgbarkeit der genannten Rechtsverletzungen aber wenigstens zu erleichtern, wird mit den vorgesehenen Maßnahmen zweifellos realisierbar sein, weshalb die zumindest abstrakte Eignung der Eingriffe des SVN-G zur Zielerreichung anzunehmen ist.¹⁷²

¹⁶⁹ Art 8 Abs 2 und Art 10 Abs 2 EMRK.

¹⁷⁰ Vgl VfGH 27.06.2014, G 47/2012 ua, Rz 165;
vgl *Hengstschläger/Leeb*, Grundrechte³ (2019) 47.
vgl EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 41-44.

¹⁷¹ Vgl EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 49.

¹⁷² Vgl VfGH 27.06.2014, G 47/2012 ua, Rz 165;
vgl EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 49.

Ob auch die Eignung zur Erreichung des zweiten im SVN-G angeführten Ziels, der „Förderung des respektvollen Umgangs der Nutzer miteinander“¹⁷³, gegeben ist, lässt sich aus juristischer Sicht schwer beurteilen, weil dieses Ziel doch eher vage geraten ist.

5.5.3 Erforderlichkeit der Eingriffsmaßnahmen des SVN-G

Auch wenn das primäre Ziel des SVN-G, die Verfolgbarkeit der genannten Rechtsverletzungen und Rechtsansprüche zu erleichtern, im öffentlichen Interesse liegen mag, und die im Entwurf konkret vorgesehenen Eingriffsmaßnahmen auch zur Erreichung dieses Ziels grundsätzlich geeignet erscheinen, so ist im nächsten Schritt zu prüfen, ob diese, insbesondere die weitreichenden Datenspeicherungs- und Übermittlungspflichten betreffend sämtliche Forennutzer, auch tatsächlich erforderlich sind, oder ob auch andere Maßnahmen verfügbar wären, die weniger intensiv in die Grundrechte der Nutzer eingreifen, aber dennoch genauso gut geeignet wären, um die mit dem Entwurf des SVN-G verfolgten Ziele zu erreichen.

Der Zweck der Verfolgung von „Hass im Netz“ nach dem Konzept einer Identifizierungspflicht für Forennutzer, wie sie das SVN-G vorsieht, ist letztendlich stets, den tatsächlichen Verfasser eines beanstandeten Kommentars ausfindig zu machen und gegebenenfalls zur Verantwortung zu ziehen. Um dies bewerkstelligen zu können, müssen jedoch nicht notwendigerweise vorab die Namen und Adressen sämtlicher Nutzer beim Forenbetreiber auf Vorrat gespeichert werden. Die österreichische Rechtsordnung ermöglicht die Rückverfolgung eines Postings auf dessen Urheber nämlich auch über andere Wege.

Oft lässt sich die Identität eines Nutzers etwa bereits über die von diesem verwendete IP-Adresse¹⁷⁴ beim betreffenden Internet-Serviceprovider (Access-Provider gemäß § 13 ECG)¹⁷⁵ ermitteln. Dies trifft jedenfalls dann zu, wenn einem bestimmten Nutzer von

¹⁷³ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 1.

¹⁷⁴ Eine IP-Adresse ist ein technischer Kommunikationsparameter, der vom Access-Provider vergeben wird, um die Endgeräte, wie Computer oder Mobiltelefon, eines bestimmten Nutzers zu adressieren und ans Internet anzubinden.

¹⁷⁵ § 13 ECG;

Ein Access-Provider stellt den Zugang zu einem Kommunikationsnetz wie beispielsweise dem Internet her oder sorgt für die Datenübermittlung in einem solchen Netz;

Zankl, E-Commerce-Gesetz. Kommentar² (2016) § 13 Rz 212.

dessen Access-Provider eine sogenannte statische IP-Adresse permanent und exklusiv zugeordnet ist. Wechselt der Access-Provider die IP-Adressen der Nutzer jedoch laufend, was meist technisch bedingt bzw aufgrund von Knappheit der verfügbaren IP-Adressen notwendig ist, dann spricht man von dynamischen IP-Adressen. In diesem Fall lässt sich nicht direkt nachvollziehen, welchem Nutzer eine bestimmte IP-Adresse zu einem konkreten Zeitpunkt zugeordnet war.¹⁷⁶

Das Gesetz bietet bereits mehrere etablierte Maßnahmen, um solche nutzerbezogenen Informationen, wie beispielsweise IP-Adressen, und mit Hilfe dieser Daten in weiterer Folge die Identität eines Forennutzers zu ermitteln. Diese Maßnahmen standen im Übrigen auch bereits zum Zeitpunkt der Veröffentlichung des Entwurfs des SVN-G zur Verfügung. An erster Stelle sind hier die in § 18 E-Commerce-Gesetz verankerten Herausgabepflichten zu nennen. Für alle Pflichten gemäß § 18 ECG gilt, dass stets nur Nutzerdaten herausgegeben werden müssen, die den Diensteanbietern durch den Betrieb ihres Dienstes ohnehin bekannt sind, es trifft sie jedoch keine Speicherpflicht oder Ermittlungspflicht.¹⁷⁷ Das bedeutet auch, dass die Diensteanbieter, anders als bei der Identifizierungspflicht des SVN-G, grundsätzlich selbst entscheiden können, welche Daten sie von ihren Nutzern einfordern und gegebenenfalls speichern. Betreiber von Diskussionsplattformen sind gemäß § 16 ECG in der Regel als sogenannte Host-Provider zu qualifizieren.¹⁷⁸

Gemäß § 18 Abs 2 ECG sind die Diensteanbieter (in diesem Fall sowohl Host-Provider als auch Access-Provider) verpflichtet, den Gerichten zum Zweck der Verfolgung von Straftaten sämtliche vorhandene Informationen zu übergeben, die sich zur Ermittlung eines Nutzers oder der Aufklärung der Tat eignen.¹⁷⁹

Auch gegenüber Verwaltungsbehörden (§ 18 Abs 3 ECG) und Dritten (§ 18 Abs 4 ECG) bestehen Pflichten zur Übermittlung von Nutzerdaten, wobei diese nur Host-Provider treffen und der Zweck hierbei jeweils nicht notwendigerweise auf die Verfolgung von Straftaten eingegrenzt ist. Stattdessen sind die Daten hier an Behörden zum Zweck der Wahrnehmung deren Aufgaben¹⁸⁰ bzw an Dritte zur Feststellung eines bestimmten rechts-

¹⁷⁶ Riesz in Riesz/Schilchegger (Hrsg), TKG. Telekommunikationsgesetz. Kommentar (2016) § 92 Rz 10.

¹⁷⁷ Zankl, E-Commerce-Gesetz. Kommentar² (2016) § 18 Rz 333.

¹⁷⁸ § 16 ECG;

Ein Host-Provider stellt im Wesentlichen Speicherplatz für fremde Informationen zur Verfügung;

Zankl, E-Commerce-Gesetz. Kommentar² (2016) § 16 Rz 258 ff.

¹⁷⁹ § 18 Abs 2 ECG.

¹⁸⁰ § 18 Abs 3 ECG.

widrigen Sachverhalts bei Nachweis eines überwiegenden rechtlichen Interesses und Glaubhaftmachung, dass die Erlangung der Information für die Rechtsverfolgung notwendig ist,¹⁸¹ auszuhändigen. Im Gegensatz zur Auskunftspflicht gegenüber Gerichten sind die Übermittlungspflichten gegenüber Behörden und Dritten jedoch jeweils eingeschränkt auf Name und Adresse der Nutzer.¹⁸² Die Rechtsprechung sieht in diesem Zusammenhang aber nicht nur die Postanschrift, sondern auch die E-Mail-Adresse eines Nutzers als vom Begriff Adresse umfasst.¹⁸³ Zur Frage, ob unter den Adressbegriff des § 18 Abs 4 ECG auch IP-Adressen fallen, liegt bisher keine Entscheidung vor, die Gesetzesmaterialien sprechen jedoch dagegen. Fest steht jedenfalls, dass zumindest dynamische IP-Adressen nicht an Privatpersonen übermittelt werden dürfen.¹⁸⁴ Darüber hinausgehende Daten müssen aber nicht ausgefolgt werden, somit, anders als im SVN-G, unter anderem auch keine Postinginhalte.¹⁸⁵ Im Gegensatz zum SVN-G drohen gemäß den Regelungen des ECG auch keine Verwaltungsstrafen oder Geldbußen für den Fall, dass ein Diensteanbieter den Auskunftspflichten gemäß § 18 ECG nicht nachkommt.¹⁸⁶ Allein deshalb ist bei Anwendung der Herausgabepflichten des ECG davon auszugehen, dass die Diensteanbieter dabei weit weniger unter Druck stehen, als dies bei Anwendung des SVN-G der Fall wäre, und sie es daher viel eher wagen würden, unzureichende Auskunftsbegehren kritisch zu hinterfragen oder abzulehnen.

Neben den Möglichkeiten des ECG existieren noch verschiedene weitergehende Auskunftspflichten in anderen Rechtsnormen, die zumeist ab einer bestimmten Mindeststrafdrohung der zu verfolgenden Straftaten anwendbar sind. Auch diese Pflichten haben gemein, dass die Diensteanbieter jeweils nur bestimmte Nutzerdaten herausgeben müssen, die sie aus eigener Entscheidung und meist zu betriebsnotwendigen Zwecken ohnehin gespeichert halten, somit besteht auch hier kein staatlich verordneter Speicherzwang. So können etwa die Sicherheitsbehörden bei Vorliegen der in § 53 Abs 3a Sicherheitspolizeigesetz (SPG) geregelten Voraussetzungen neben den Stammdaten zu-

¹⁸¹ § 18 Abs 4 ECG.

¹⁸² § 18 Abs 3 und Abs 4 ECG.

¹⁸³ *Zankl*, E-Commerce-Gesetz. Kommentar² (2016) § 18 Rz 348;
Zankl, E-Commerce-Gesetz. Kommentar² (2016) § 18 Rz 364;
RIS-Justiz RS0127160.

¹⁸⁴ *Anderl*, Kein Auskunftsanspruch bei dynamischer IP-Adresse, *ecolex* 2012/367, 904 (905);
OGH 22.06.2012, 6 Ob 119/11k.

¹⁸⁵ *Zankl*, E-Commerce-Gesetz. Kommentar² (2016) § 18 Rz 364.

¹⁸⁶ *Zankl*, E-Commerce-Gesetz. Kommentar² (2016) § 18 Rz 365.

sätzlich die Übermittlung der IP-Adresse eines Forennutzers vom Diensteanbieter verlangen, dies umfasst sowohl statische als auch dynamische IP-Adressen.¹⁸⁷ Auch § 76a Strafprozessordnung (StPO) bietet kriminalpolizeilichen Behörden, Staatsanwaltschaften und Gerichten die Möglichkeit, Stammdaten eines bestimmten Nutzers, gegen den sich der konkrete Verdacht einer Straftat richtet, von den Kommunikationsdiensteanbietern herauszuverlangen.¹⁸⁸ Gemäß § 76a Abs 2 StPO kann die Staatsanwaltschaft zudem sogar die Offenlegung von Name und Anschrift jenes Nutzers anordnen, dem zu einem konkreten Zeitpunkt eine bestimmte dynamische IP-Adresse zugeteilt war, vorausgesetzt, dass hierfür kein größerer Personenkreis in Frage kommt.¹⁸⁹

Wie erläutert, ist es bei all diesen Maßnahmen jeweils nicht notwendig, die Nutzer, die sich in den Foren eventuell strafbar machen könnten, vorab zu registrieren. Stattdessen greifen diese Mittel erst dann ein, wenn auch tatsächlich bereits ein Tatverdacht vorliegt. Der Annahme, dass die Identitätsermittlung von Forennutzern mit den bestehenden Auskunftspflichten mangels gespeicherter Nutzerdaten oder aufgrund von vom Nutzer angegebener Phantasiedaten zu oft scheitern würde, lassen sich praktische Erfahrungswerte gegenüberstellen. So lässt sich in sozialen Netzwerken wie Facebook die Identität von Tätern zumeist schon deshalb relativ einfach ermitteln, da diese oft viele persönliche Informationen von sich in ihrem Profil öffentlich preisgeben.¹⁹⁰ Nicht übersehen werden darf außerdem, dass sehr viele Verfasser von Hasspostings diese ohnehin unter Verwendung ihrer bürgerlichen Namen veröffentlichen, wie Erfahrungen aus der Praxis zeigen.¹⁹¹

¹⁸⁷ § 53 Abs 3a SPG;

Zankl, E-Commerce-Gesetz. Kommentar² (2016) § 18 Rz 347;

Reindl-Krauskopf/Salimi/Stricker, IT-Strafrecht, Rz 5.206 ff (Stand 01.09.2018, rdb.at).

¹⁸⁸ § 76a StPO.

¹⁸⁹ § 76a Abs 2 StPO;

Reindl-Krauskopf/Salimi/Stricker, IT-Strafrecht, Rz 5.52 f (Stand 01.09.2018, rdb.at).

¹⁹⁰ *Brodnig*, Hass im Netz. Was wir gegen Hetze, Mobbing und Lügen tun können (2016) 167.

¹⁹¹ *Wimmer*, Studie: Klarnamen verhindern keine Hasspostings, Website Futurezone 13.01.2021

<futurezone.at/science/studie-klarnamen-verhindern-keine-hasspostings/211.959.224>

(abgefragt am 14.01.2022);

Lang, Rassist:innen kommentieren mit identifizierbaren Accounts, Website netzpolitik.org 12.08.2021

<www.netzpolitik.org/2021/anonymitaet-im-netz-rassistinnen-komentieren-mit-identifizierbaren-accounts> (abgefragt am 14.01.2022);

blog.twitter.com, Website 19.02.2021, No room for racist behaviour on Twitter

<blog.twitter.com/en_gb/topics/company/2020/no-room-for-racist-behaviour-on-twitter->

(abgefragt am 14.01.2022).

Es ist daher schon prinzipiell in Frage zu stellen, ob die im SVN-G vorgesehene Registrierung sämtlicher Forennutzer mit Name und Adresse und die Übermittlung dieser personenbezogenen Daten an ansuchende Gerichte, Strafverfolgungsbehörden oder sogar Privatpersonen und privatrechtliche Unternehmen überhaupt erforderlich ist, oder ob ein Zurückgreifen auf die bereits bestehenden Werkzeuge der Rechtsordnung zur Ermittlung der Identität von Nutzern nicht als jeweils gelinderes Mittel zu werten wäre.

5.6 Adäquanz - Verhältnismäßigkeit im engeren Sinn

Die Verhältnismäßigkeit der verwirklichten Grundrechtseingriffe kann nur dann gewährleistet werden, wenn die Auswirkungen des jeweiligen Eingriffs auf den Schutzbereich nicht schwerer wiegen als die Relevanz und Tragweite der mit dem Eingriff angestrebten Ziele.¹⁹² Es ist somit eine Abwägung der Schwere der durch die Maßnahmen des SVN-G bewirkten Grundrechtseingriffe mit der Bedeutung der mit dem SVN-G verfolgten Ziele vorzunehmen. Dabei ist es auch notwendig, dass die gewählten Eingriffsmaßnahmen bei einer staatlich angeordneten Sammlung von Daten das jeweils gelindeste Mittel darstellen, welches zur Verfügung steht, um das im öffentlichen Interesse gelegene Ziel zu erreichen.¹⁹³

Auch bei der Prüfung der Verhältnismäßigkeit der Eingriffe des SVN-G kann, aufgrund der großen Überschneidungen, wieder in zahlreichen konkreten Detailfragen auf die bisherige höchstgerichtliche Rechtsprechung zur Vorratsdatenspeicherung zurückgegriffen werden. Schließlich verfolgen das SVN-G und die Vorratsdatenspeicherung von Telekommunikationsdaten im Grunde dieselben Ziele, nämlich die Aufrechterhaltung der öffentlichen Ordnung und Sicherheit und den Schutz der Rechte anderer.¹⁹⁴ Zudem sind die die Eingriffe ermöglichenden Maßnahmen jeweils, sowohl was Art und Umfang der zu sammelnden personenbezogenen Daten, als auch die Größe des betroffenen Personenkreises anbelangt, sehr ähnlich. Auch das SVN-G müsste demzufolge, entsprechend des Standpunkts des EuGH zur Vorratsdatenspeicherung, „klare und präzise Regeln für die

¹⁹² Vgl VfGH 27.06.2014, G 47/2012 ua, Rz 166.

¹⁹³ *Mayer/Kucsko-Stadlmayer/Stöger*, Grundriss des österreichischen Bundesverfassungsrechts¹¹ (2015) Rz 1340;

Berka, Öffentliches Recht. Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT I/1 (2012) 115 f.

¹⁹⁴ Vgl VfGH 27.06.2014, G 47/2012 ua, Rz 165.

Tragweite und die Anwendung der fraglichen Maßnahme vorsehen und Mindestanforderungen aufstellen, so dass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen“¹⁹⁵.

Der VfGH hat Bedeutung und Gewicht der mit der Vorratsspeicherung von Telekommunikationsdaten verfolgten Ziele zwar als erheblich und als einem wichtigen öffentlichen Interesse dienend qualifiziert, dabei jedoch aufgrund der aus der „Streubreite“ des Eingriffs, des Kreises und der Art der betroffenen Daten resultierenden Schwere des Eingriffs klargestellt, dass die bei der Vorratsspeicherung herangezogenen Daten nur unter Anwendung besonderer Absicherungsmaßnahmen zugänglich gemacht werden dürfen. Der VfGH verlangt vom Gesetzgeber als solche spezifische Garantie zur Sicherstellung der Verhältnismäßigkeit derart weitreichender Eingriffe, dass die Daten nur dann einem Berechtigten ausgehändigt werden, wenn eine der richterlichen Kontrolle unterliegende Einzelfallüberprüfung ergibt, dass in jedem konkreten Fall auch tatsächlich ein gewichtiges öffentliches Interesse vorliegt.¹⁹⁶ Ob das SVN-G derartige Garantien enthält und die einzelnen Eingriffsmaßnahmen entsprechend dieser Vorgaben im Vergleich zu den angestrebten Zielen tatsächlich verhältnismäßig sind, soll in den folgenden Schritten im Detail untersucht werden.

5.6.1 Maßnahmen sind nur zur Verfolgung schwerer Straftaten zulässig

Zunächst ist festzustellen, dass das SVN-G zwar unter der Parole des „Kampfs gegen Hass im Netz“ vermarktet wurde, es jedoch tatsächlich ein Strafverfolgungswerkzeug darstellt, das sich nicht bloß auf die Verfolgung klassischer Hasskommentare beschränkt, sondern viel umfassender einsetzbar ist. Als zentrale Pflicht sieht das SVN-G vor, dass betroffene Diensteanbieter wegen des Verdachts jedes erdenklichen strafrechtlich relevanten, egal ob vorsätzlichen oder fahrlässigen Verhaltens die personenbezogenen Daten eines Nutzers an kriminalpolizeiliche Behörden, Staatsanwaltschaften und Gerichte übermitteln müssen.¹⁹⁷ Denn das SVN-G ordnet die Herausgabe der Nutzerdaten lediglich für den allgemein gehal-

¹⁹⁵ EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 54.

¹⁹⁶ VfGH 27.06.2014, G 47/2012 ua, Rz 168.

¹⁹⁷ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 4 Abs 3.

tenen Zweck der „Strafverfolgung“ an, nimmt hierbei aber keine Eingrenzung auf bestimmte Delikte vor.¹⁹⁸ Somit haben die genannten Behörden und Gerichte die Möglichkeit, bereits wegen des Verdachts geringster strafrechtlich relevanter Verstöße die Herausgabe der Nutzerdaten zu verlangen. Eine Einschränkung auf konkrete Straftatbestände, die typischerweise mit der Verbreitung von Hasskommentaren assoziiert werden, besteht dabei in keiner Weise. Nur für Auskunftsbegehren von Dritten, also von Privatpersonen und Unternehmen, grenzt das SVN-G die Herausgabe der Daten dahingehend ein, auf das Vorliegen des Verdachts bestimmter taxativ aufgezählter Privatanklagedelikte und auf die zivilrechtlichen Ansprüche wegen Ehrenbeleidigung und Kreditschädigung gemäß § 1330 ABGB.¹⁹⁹

Der VfGH hat im Erkenntnis zur Vorratsdatenspeicherung festgestellt, dass durch einen gesetzlich vorgesehenen Eingriff nur zur Verfolgung schwerer Straftaten auf Vorratsdaten zugegriffen werden darf. Darüber hinaus hält er fest, dass der Gesetzgeber sicherzustellen hat, dass die Schwere der anlassgebenden Straftat auch im konkreten Einzelfall den Eingriff in die Grundrechte der betroffenen Person tatsächlich rechtfertigt.²⁰⁰

Auch der EuGH gelangt im Urteil *Tele2 Sverige* zur Ansicht, dass aufgrund der gebotenen Verhältnismäßigkeit, in Anbetracht der Schwere des mit einem derartigen Gesetz bewirkten Grundrechtseingriffs, nur die Verfolgung von schweren Straftaten gerechtfertigt sein kann.²⁰¹ Zudem hat der EuGH im selben Urteil erkannt, dass ein Eingriff in die Vertraulichkeit der Kommunikation durch ein nationales Gesetz, welches zu Strafverfolgungszwecken den Zugang zu auf Vorrat gespeicherten Daten eröffnet, schon grundsätzlich als schwerwiegender Eingriff zu werten ist.²⁰²

Auch das SVN-G, das demselben Prinzip wie die in den genannten grundlegenden Entscheidungen zur Vorratsdatenspeicherung gegenständlichen Rechtsnormen folgt, stellt ein solches nationales Gesetz dar, das durch die Ermöglichung des Zugriffs auf Vorratsdaten einen Eingriff in die Vertraulichkeit der Kommunikation bewirkt. Daraus folgt, dass auch der durch das SVN-G bewirkte Eingriff als schwerwiegender Eingriff zu qualifizieren ist. Um einen Eindruck zu gewinnen, was in diesem Zusammenhang unter „schweren Straftaten“ zu verstehen ist, bietet sich ein Blick auf die vom EuGH aufgehobene

¹⁹⁸ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 4.

¹⁹⁹ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 4 Abs 2.

²⁰⁰ VfGH 27.06.2014, G 47/2012 ua, Rz 171.

²⁰¹ EuGH 21.12.2016, C-203/15, C-698/15 (*Tele2 Sverige* und *Watson u.a.*) Rz 115.

²⁰² EuGH 21.12.2016, C-203/15, C-698/15 (*Tele2 Sverige* und *Watson u.a.*) Rz 115.

Vorratsdatenspeicherungsrichtlinie vom 15.03.2006 an. Diese Richtlinie sah nämlich explizit vor, dass die davon umfassten Vorratsdaten nur „zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten“²⁰³ zu speichern waren. Wie sich aus den Materialien zur Richtlinie entnehmen lässt, hat der europäische Gesetzgeber bei Verwendung des Begriffs der schweren Straftat in erster Linie terroristische Straftaten im Sinn gehabt.²⁰⁴ Im Gegensatz dazu sind vom Anwendungsbereich des SVN-G jedoch, wie erläutert, sämtliche Straftaten umfasst, also auch bereits leichteste Vergehen. Einschränkungen auf eine gewisse Schwere, geschweige denn Taten mit terroristischem Hintergrund, sucht man vergeblich.

Auch beim SVN-G ist daher zum einen das Abstellen auf eine bestimmte Schwere der Straftat erforderlich. Zudem muss auch hier im konkreten Einzelfall eine Abwägung der Schwere der konkreten Straftat und dem Gewicht des jeweiligen Grundrechtseingriffs vorgenommen werden. Das gänzliche Fehlen einer adäquaten Erheblichkeitsschwelle ist, gemessen an der Rechtsprechung des VfGH und des EuGH, ein deutliches Indiz für die Unverhältnismäßigkeit der Maßnahmen des SVN-G.²⁰⁵

5.6.2 Betroffener Personenkreis zu weit gefasst

Ebenso wie bei der Vorratsdatenspeicherung von Telekommunikationsdaten kommt es auch im Fall des SVN-G zu einer massenhaften, systematischen Speicherung von personenbezogenen Daten sämtlicher Nutzer. Diese Speicherung erfolgt unterschiedslos und ausnahmslos für alle Nutzer der vom SVN-G betroffenen Diskussionsplattformen. Damit sind von den Maßnahmen aber unweigerlich auch zahlreiche Personen mitbetroffen, bei denen nicht die geringsten Anzeichen vorliegen, dass diese durch die Nutzung des Online-dienstes je ein Verhalten setzen werden, das strafrechtlich zu ahnden wäre.²⁰⁶

Da sich die vom SVN-G umfassten Onlinedienste, zu denen auch globale Social-Media-Plattformen wie Facebook zählen, reger Beliebtheit erfreuen, ist davon auszugehen, dass außerordentlich viele Menschen in Österreich von den Maßnahmen des SVN-G betroffen wären. Allein Facebook, das angibt, weltweit aktuell etwa 2,5 Milliarden Nutzer vorweisen

²⁰³ Art 1 Abs 1 Vorratsdatenspeicherung-RL 2006/24 ABl L 2006/105, 54.

²⁰⁴ ErwGr 8-10 Vorratsdatenspeicherung-RL 2006/24 ABl L 2006/105, 54.

²⁰⁵ Vgl VfGH 11.12.2019, G 72-74/2019, G 181-182/2019, Rz 103 ff.

²⁰⁶ Vgl EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 58.

zu können,²⁰⁷ beruft sich in Österreich auf 3,9 Millionen aktive Nutzer pro Monat. 3 Millionen Österreicher sollen Facebook sogar täglich verwenden.²⁰⁸ Die größte Diskussionsplattform eines österreichischen Anbieters ist das Online-Forum der Tageszeitung „Der Standard“, in dem laut eigenen Angaben täglich bis zu 40.000 Nutzerkommentare veröffentlicht werden.²⁰⁹ Diese Zahlen verdeutlichen, dass die Anzahl der von den Eingriffen des SVN-G betroffenen Bürger tatsächlich beträchtlich wäre. Im Vergleich dazu steht die Zahl der Personen, die bei der Nutzung der betroffenen Online-dienste erwartbarerweise tatsächlich Straftaten begehen könnten, in keiner Relation. Im Ergebnis sind damit, ebenso wie es bei der Vorratsdatenspeicherung von Telekommunikationsdaten der Fall war, angesichts der Masse an betroffenen Bürgern, auch vom SVN-G fast ausschließlich Personen erfasst, die einerseits unbescholten sind und zudem nicht den geringsten Anlass dafür geben, dass ihre personenbezogenen Daten zum Zweck der Bekämpfung von Straftaten oder der im SVN-G angeführten zivilrechtlichen Verstöße gespeichert werden müssten. Hinsichtlich dieser überwältigenden Mehrheit wiegen die durch das Gesetz verursachten Grundrechtseingriffe besonders schwer.²¹⁰

Als entscheidend stellt sich auch das gänzliche Fehlen einer Anlassbezogenheit der Datenverarbeitungsmaßnahmen des SVN-G dar. Die Setzung einer solchen Schranke wäre förderlich, um den betroffenen Personenkreis auf ein akzeptables Maß zu reduzieren. Da eine Maßnahme wie das SVN-G grundsätzlich nur zur Verfolgung von schweren Straftaten denkbar ist, wäre eine Eingrenzung der Anwendung etwa auf Nutzer, die in der Vergangenheit bereits schwere Straftaten verwirklicht haben oder aktuell konkret unter Verdacht stehen, in eine solche schwere Straftat involviert zu sein, eine mögliche Abmilderung.²¹¹ Praktisch umsetzbar wäre eine solche Einschränkung jedoch wohl nur, indem man nur die

²⁰⁷ Die Presse, Website 30.01.2020, Facebook wächst auf 2,5 Milliarden Nutzer <www.diepresse.com/5760750/facebook-wachst-auf-25-milliarden-nutzer> (abgefragt am 14.01.2022).

²⁰⁸ Roth, Offizielle Facebook Nutzerzahlen für Deutschland (Stand: März 2019), Website allfacebook.de 19.03.2019 <www.allfacebook.de/zahlen_fakten/offiziell-facebook-nutzerzahlen-deutschland> (abgefragt am 14.01.2022).

²⁰⁹ Kotynek, Gegen Hass im Netz sind Klarnamen keine Lösung, Website Der Standard 04.01.2019 <www.derstandard.at/story/2000095399328/klarnamen-sind-keine-loesung> (abgefragt am 14.01.2022).

²¹⁰ Vgl VfGH 27.06.2014, G 47/2012 ua, Rz 183 f;
vgl EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 58.

²¹¹ Vgl EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 59.

Herausgabe der Daten einer Person zulassen würde, die einer schweren Straftat konkret verdächtigt wird, wie es der EuGH in der Entscheidung *Tele2 Sverige* unter Verweis auf das Urteil des EGMR vom 04.12.2015 (*Roman Zakharov gg Russland*) angedacht hat.²¹² Dies würde aber erfordern, dass dennoch zuvor die personenbezogenen Daten aller Foren-
nutzer gesammelt und auf Vorrat gespeichert werden müssten, was wiederum auch Eingriffe in die Grundrechte jedes einzelnen Nutzers bedeuten würde. Somit wäre zwar betreffend die Herausgabe der Nutzerdaten eine Einschränkung auf einzelne Personen theoretisch denkbar, eine umfassende Reduzierung des betroffenen Personenkreises auf ein verhältnismäßiges Maß wäre bei einer Identifizierungspflicht wie dem SVN-G aber wohl schon allein aus praktischen Gründen gar nicht möglich. So kann, wie schon bei der Vorratsdatenspeicherung von Telekommunikationsdaten, der Anschein entstehen, dass der Gesetzgeber die Nutzer gewissermaßen unter Generalverdacht stellt.

5.6.3 Gefahr des Datenmissbrauchs und des unbefugten Zugriffs

Es besteht eine erhebliche Gefahr der missbräuchlichen Verwendung und des unbefugten Zugriffs auf die massenhaft zu speichernden Nutzerdaten. Die Gründe dafür liegen vor allem in der Art der Daten selbst, aber auch im mitunter großen und nur schwer überblickbaren Kreis der zur Speicherung verpflichteten Diensteanbieter, was dazu führt, dass eine Vielzahl an Personen potentiell Zugriff auf die Daten hat.²¹³

Das Missbrauchspotential zeigt sich einerseits darin, dass die in Anwendung des SVN-G zu speichernden Nutzerdaten einen großen wirtschaftlichen Wert verkörpern. Vor allem die Inhalte der Postings, in denen die Nutzer ihre persönliche Meinung offen kundtun, stellen eine für bestimmte Wirtschaftszweige unbezahlbare Informationsquelle dar. So ließen sich etwa durch Verknüpfung der gespeicherten Daten, also der in den Postinginhalten gesammelten persönlichen Ansichten eines bestimmten Nutzers und dessen Name und Adresse, sehr einfach auf die persönlichen Vorlieben dieser Person maßgeschneiderte Werbeangebote erstellen. Die Daten wären aber beispielweise auch für den Marktforschungsbereich oder die Erstellung politischer Umfragen von großem Wert, da man

²¹² Vgl. EuGH 21.12.2016, C-203/15, C-698/15 (*Tele2 Sverige* und *Watson u.a.*) Rz 119, der EuGH verweist hier auf EGMR 04.12.2015, 47143/06 (GK) (*Roman Zakharov gg Russland*) Rz 260.

²¹³ Vgl. VfGH 27.06.2014, G 47/2012 ua, Rz 187.

anhand der Nutzerdaten die Ansichten bestimmter Bürger ohne großen Aufwand katalogisieren könnte. Solche Verfahren werden auch jetzt bereits angewendet, wie ein im Jahr 2019 bekanntgewordener Fall zeigt, bei dem die Österreichischen Post AG Datensätze zum Kauf angeboten hat, in denen betroffenen Personen durch Verschneidung gesammelter personenbezogener Daten eine mutmaßliche Affinität zu bestimmten politischen Parteien zugeschrieben wurde.²¹⁴ Unter Anwendung des SVN-G könnte man die politische Ausrichtung von Bürgern aber noch wesentlich exakter ermitteln, da die Nutzer in Diskussionsforen häufig ganz offen preisgeben, welche politische Meinung sie präferieren.

Vom Anwendungsbereich des SVN-G können unterschiedlichste Onlinedienste betroffen sein, sofern diese auch eine Diskussionsplattform anbieten. Für Personen, die im Netz besonders aktiv und daher in vielen verschiedenen Foren oder sozialen Netzwerken registriert sind, hat das zur Folge, dass auch dementsprechend viele unterschiedliche Diensteanbieter ihre personenbezogenen Daten speichern müssen. Dies kann bewirken, dass Nutzer schlicht den Überblick darüber verlieren, welche Diensteanbieter ihre persönlichen Daten gespeichert haben. Hinzu kommt, dass die Diensteanbieter die Daten zur Erfüllung der Verpflichtungen des SVN-G dauerhaft, also ohne Befristung speichern müssen, solange ein Nutzer im Forum aktiv bleibt. Je mehr verschiedene Diensteanbieter personenbezogene Daten eines Nutzers aufbewahren, desto mehr Personen haben auch potentiell Zugriff auf diese. Das erhöht unweigerlich auch die Missbrauchsgefahr.²¹⁵

Bereits § 1 Abs 2 DSG bestimmt, dass gesetzliche Eingriffe in das Grundrecht auf Datenschutz, vor allem wenn diese die Verwendung von besonders schutzwürdigen Daten umfassen, „angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen“²¹⁶ festlegen müssen. Um dem zu entsprechen, müsste der Gesetzgeber Maßnahmen im SVN-G vorsehen, die dem Missbrauch der Nutzerdaten durch die verpflichteten Diensteanbieter selbst oder durch auskunftsberechtigte Stellen, denen die Daten übermittelt worden sind, vorbeugen. Für dennoch auftretende Fälle von missbräuchlicher Verwendung müsste der Gesetzgeber, entsprechend der Ansicht des VfGH, auch Strafen für die verantwortlichen Diensteanbieter vorsehen.²¹⁷

²¹⁴ *Hametner/Mayrhofer/Müller/Zirnig*, Wenn die Post Partei ergreift, Website Addendum 07.01.2019 <www.addendum.org/datenhandel/parteiaffinitaet> (abgefragt am 14.01.2022).

²¹⁵ Vgl VfGH 27.06.2014, G 47/2012 ua, Rz 187.

²¹⁶ § 1 Abs 2 DSG.

²¹⁷ Vgl VfGH 27.06.2014, G 47/2012 ua, Rz 187.

Der Entwurf des SVN-G hingegen scheint diese Missbrauchsgefahren völlig auszublenden. Er enthält praktisch keine Sicherheitsvorkehrungen, ebenso fehlen Strafen für Datenmissbrauch durch Diensteanbieter oder gemäß SVN-G auskunftsberechtigte Stellen und Personen. Der Entwurf enthält zwar Strafbestimmungen, diese dienen jedoch ganz anderen Zwecken, da diese lediglich die Nichteinhaltung der Pflichten zur Identifizierung der Forennutzer durch die Diensteanbieter pönalisieren, aber nicht einen Datenmissbrauch.²¹⁸ Des Weiteren müsste im Gesetz auch geregelt sein, wer letztendlich Zugang zu den Daten haben darf. Die Anzahl der zugangsberechtigten Personen müsste dabei auf das absolut notwendige Mindestmaß beschränkt werden.²¹⁹

5.6.4 Materiell- und verfahrensrechtliche Regeln für den Zugang zu den Daten

Ein weiterer Mangel im Hinblick auf die Einschränkung der Eingriffe auf das absolut Notwendige besteht darin, dass das SVN-G keine materiell- und verfahrensrechtlichen Bestimmungen enthält, die beispielsweise den genauen Ablauf der Interaktion zwischen den Diensteanbietern und den auskunftsberechtigten Gerichten, Behörden und Dritten regeln. Insbesondere fehlt auch ein klar definierter Prozess, der vorgibt, wie der Zugang der Auskunftsberechtigten zu den Daten zu erfolgen hat und zu welchen Zwecken und in welchem Umfang die spätere Nutzung der Daten gestattet ist.²²⁰ Angesichts der Sensibilität der zu verarbeitenden personenbezogenen Daten wären hierzu klare Vorschriften dringend angebracht. Diese Verfahrensregeln müssten idealerweise auch exakt vorgeben, auf welchem Kommunikationsweg Gerichte, Behörden und Dritte mit dem Diensteanbieter in Kontakt zu treten haben. Dies wäre nicht nur zur Vermeidung von Missbrauch geboten, sondern auch, weil der Diensteanbieter darüber hinaus mit der Pflicht konfrontiert ist, die Zulässigkeit der Ansuchen von Dritten selbst prüfen zu müssen.²²¹

Da im SVN-G entsprechende Vorschriften fehlen, muss damit gerechnet werden, dass betroffene Diensteanbieter jeweils eigene Prozesse zur Abwicklung ihrer Pflichten aus dem SVN-G, insbesondere für den Ablauf der Kommunikation und der Datenübermittlung

²¹⁸ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, §§ 7 und 8.

²¹⁹ Vgl. EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 62.

²²⁰ Vgl. EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 61.

²²¹ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 4 Abs 2.

schaffen würden. Stattdessen wäre aber ein für alle betroffenen Diensteanbieter vereinheitlichtes Verfahren sinnvoll, da so weitere Rechtsunsicherheiten vermieden werden könnten. Da der Diensteanbieter die Verantwortung für die Herausgabe der personenbezogenen Nutzerdaten trägt, muss er sich gewiss sein können, dass der Ansuchende auch tatsächlich gemäß den Bestimmungen des SVN-G legitimiert ist, die Daten übermittelt zu bekommen. Bei Dritten, also Privatpersonen und privatrechtlichen Unternehmen, hätte der Diensteanbieter zudem auch sorgfältig zu prüfen, ob bei diesen ein „begründetes Verlangen“ im Sinne des § 4 Abs 1 SVN-G vorliegt.²²²

Gerichte, Behörden und Dritte müssten den Betroffenen zudem nachträglich informieren, wenn seine Nutzerdaten an sie herausgegeben worden sind und auch bekanntgeben, um welche Daten es sich genau handelt, sobald dies die Ermittlungen nicht mehr gefährdet. Diese Information hat unter anderem deshalb zu erfolgen, um dem Betroffenen die Möglichkeit einzuräumen, Rechtsmittel erheben zu können.²²³ Die Information des Betroffenen über eine erfolgte Datenübermittlung wäre auch angesichts der allenfalls zahlreichen Diensteanbieter, die personenbezogene Daten des Betroffenen speichern müssen, angebracht. Viele Internetnutzer sind typischerweise bei mehreren Onlinediensten oder Social-Media-Plattformen registriert, von denen sie einige eventuell nur selten verwenden. So ist damit zu rechnen, dass manchen Nutzern schlicht der Überblick fehlt, welche Diensteanbieter ihre Nutzerdaten gespeichert halten.

Da der Entwurf keine derartigen Informationspflichten vorsieht, würden damit sowohl die Herausgabe der Nutzerdaten als auch die Ermittlungen selbst wohl meist stattfinden, ohne dass der Betroffene zeitnah davon erfährt. Der betroffene Nutzer kann jedoch ohne Kenntnis von der erfolgten Herausgabe seiner personenbezogenen und mitunter sensiblen Daten auch kein Rechtsmittel, wie etwa Beschwerde an die Datenschutzbehörde gemäß § 24 DSG, erheben.²²⁴ Der Entwurf des SVN-G sieht auch keinerlei eigenständige Rechtsbehelfe für Betroffene vor, die eine zielgerichtete Anfechtung von bereits erfolgten Maßnahmen ermöglichen.

²²² ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 4 Abs 1 und 2.

²²³ Vgl EuGH 21.12.2016, C-203/15, C-698/15 (*Tele2 Sverige* und *Watson u.a.*) Rz 121.

²²⁴ Vgl VfGH 11.12.2019, G 72-74/2019, G 181-182/2019, Rz 105.

5.6.5 Vorprüfung und Kontrolle durch Gericht oder unabhängige Behörde

Auch wenn das SVN-G grundsätzlich ein im öffentlichen Interesse liegendes Ziel verfolgt, stellen dessen Maßnahmen gravierende Grundrechtseingriffe dar. Die Intensität der Eingriffe resultiert unter anderem aus dem großen Kreis an betroffenen Personen, der Art und Sensibilität der zu verarbeitenden Daten und insbesondere der Möglichkeit, aus den Nutzerdaten Rückschlüsse auf die Lebensführung, persönlichen Ansichten, privaten Vorlieben und den Bekanntenkreis der Nutzer zu gewinnen. Der Gesetzgeber hat daher, gemäß der Rechtsprechung des VfGH, zwingend zu garantieren, „dass diese Daten nur bei Vorliegen eines vergleichbar gewichtigen öffentlichen Interesses im Einzelfall für Strafverfolgungsbehörden zugänglich gemacht werden und dies einer richterlichen Kontrolle unterliegt.“²²⁵

Die Einhaltung der bei Grundrechtseingriffe ermöglichenden Rechtsnormen wie dem SVN-G notwendigen materiell- und verfahrensrechtlichen Voraussetzungen für den Zugang zu den Nutzerdaten, die im Entwurf des SVN-G jedoch weitgehend fehlen, sowie die Überprüfung der Anträge auf Datenherausgabe auf deren Rechtmäßigkeit, bedarf somit, entsprechend der Rechtsprechung der Höchstgerichte, der zwingenden Vorprüfung eines Gerichts oder einer unabhängigen Behörde. Auch der Zugriff auf Vorratsdaten darf nur unter richterlicher Kontrolle erfolgen. Anträge auf Herausgabe von auf Vorrat gespeicherten Nutzerdaten müssen zudem begründet sein und die konkreten Straftatbestände nennen, aufgrund derer die jeweilige Ermittlungsmaßnahme für notwendig erachtet wird.²²⁶ Diese Grundvoraussetzung wird vom SVN-G allerdings gänzlich ignoriert.

Die Prüfung der erforderlichen Voraussetzungen für eine Datenübermittlung durch ein Gericht oder eine unabhängige Behörde ist auch deshalb notwendig, weil diese Aufgabe, anders als im SVN-G vorgesehen, nicht den Diensteanbietern auferlegt werden sollte. Der Gesetzesentwurf bestimmt nämlich, dass die Diensteanbieter selbst die Anträge auf Datenherausgabe auf deren rechtliche Zulässigkeit und das Vorliegen der notwendigen Voraussetzungen zu prüfen haben.²²⁷ Dabei handelt es sich um eine rechtliche Beurteilung,

²²⁵ VfGH 27.06.2014, G 47/2012 ua, Rz 168.

²²⁶ Vgl EuGH 21.12.2016, C-203/15, C-698/15 (*Tele2 Sverige* und *Watson u.a.*) Rz 120; vgl VfGH 27.06.2014, G 47/2012 ua, Rz 168 u 175; vgl VfGH 11.12.2019, G 72-74/2019, G 181-182/2019, Rz 105.

²²⁷ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 4.

und damit um eine Aufgabe, die nicht vom Staat auf privatrechtliche Unternehmen abgewälzt werden sollte.

Um entscheiden zu können, ob das Vorliegen eines „begründeten Verlangens“²²⁸ im Sinne von § 4 Abs 1 SVN-G, eines „konkreten Verdachts einer durch den Inhalt eines Postings begangenen Straftat des Posters“²²⁹ im Sinne von § 4 Abs 3 SVN-G oder von „begründeten Hinweisen, [...] dass der Inhalt [eines Postings - *Anm. d. Verf.*] sonst den konkreten Verdacht einer Straftat begründen könnte“²³⁰ im Sinne von § 4 Abs 4 SVN-G, gegeben ist, welches zur Herausgabe der Nutzerdaten bzw der Postinginhalte verpflichtet, bedarf es nämlich auch einer gewissen Auseinandersetzung mit den Tatbestandselementen der behaupteten Straftaten. Weil es sich bei den Dienstnehmern der Diensteanbieter aber wohl meist eher um juristische Laien handeln wird und auch die Unabhängigkeit ihrer Entscheidung nicht gewährleistet ist, erweist sich eine Vorprüfung durch die Diensteanbieter selbst als problematisch. Entscheidet der Diensteanbieter, dass er eine Übermittlung von Nutzerdaten an den Ansuchenden durchführt, ist zu beachten, dass dieser Übermittlungsvorgang, nach der vorangegangenen Speicherung und Verarbeitung der Nutzerdaten, auch einen weiteren Grundrechtseingriff darstellt.²³¹ Die Verantwortung, über die Durchführung dieses weiteren Grundrechtseingriffs zu entscheiden, sollte nicht dem Diensteanbieter als „Privaten“ aufgebürdet werden.

Ein weiterer Grund für die Notwendigkeit der Vorprüfung durch ein Gericht ergibt sich daraus, dass die Diensteanbieter gemäß § 4 Abs 4 SVN-G verpflichtet sind, zusätzlich zu den Personalien eines Nutzers auch Aufzeichnungen bestimmter Postinginhalte an den Ansuchenden herauszugeben.²³² Postinginhalte sind, wie erläutert, besonders sensibel, da diese direkte Rückschlüsse auf die Gedankenwelt eines Nutzers zulassen. Der dahingehenden Interpretation des SVN-G-Entwurfs zufolge müssen die Diensteanbieter selbst solche Kommentare an Ansuchende herausgeben, die in einem geschlossenen Forumsbereich gepostet wurden, also in einem Bereich, in dem der Ansuchende selbst eventuell

²²⁸ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 4 Abs 1.

²²⁹ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 4 Abs 3.

²³⁰ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 4 Abs 4.

²³¹ Vgl EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 35.

²³² ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 4 Abs 4.

gar keine Leseberechtigung hat.²³³ Dies birgt wiederum ein gewisses Missbrauchspotential, indem jemand etwa unter Behauptung einer Rechtsverletzung die Herausgabe eines ihm gar nicht bekannten Postings verlangen könnte, nur mit dem Ziel, an nicht für ihn bestimmte vertrauliche Informationen zu gelangen, die ein Nutzer in ein geschlossenes Forum gestellt hat. Da die Herausgabe von Postinginhalten aus einem geschlossenen Forum jedoch einen Eingriff in das Fernmeldegeheimnis darstellen kann, müsste gemäß Art 10a StGG hierfür ohnehin zwingend ein richterlicher Befehl oder eine gerichtliche Genehmigung vorliegen.²³⁴

Unterläuft dem Diensteanbieter bei der ihm aufgetragenen Prüfung der Ansuchen ein Fehler, so ist anzunehmen, dass der Diensteanbieter dem betroffenen Nutzer für die Folgen der dann möglicherweise rechtswidrigen Herausgabe der Nutzerdaten haftet, etwa wenn sich herausstellt, dass der Antragsteller gar nicht berechtigt war, die Daten vom Diensteanbieter übermittelt zu bekommen. Auch dieses Problem könnte durch einen Richtervorbehalt entschärft werden.

5.6.6 Gefahr des „Overblocking“

Dass das SVN-G die Pflicht zur Überprüfung der Anträge und damit die Entscheidung über die Herausgabe der Nutzerdaten und Postinginhalte den Diensteanbietern abverlangt, anstatt dies dazu befähigten Gerichten oder unabhängigen Behörden zu überlassen, bringt noch eine weitere, besonders schwerwiegende Problematik mit sich: Insbesondere aufgrund der drohenden, empfindlichen Strafen bei Nichtbefolgung ist zu befürchten, dass die Diensteanbieter sich so sehr unter Druck gesetzt fühlen könnten, dass sie im Zweifel dazu tendieren würden, selbst unzureichende Anträge auf Übermittlung von Nutzerdaten eher zu

²³³ Das SVN-G trifft keine Unterscheidung zwischen für prinzipiell jedermann öffentlich zugänglichen Foren und nur einem geschlossenen Kreis von Berechtigten zugänglichen Plattformen. Der Entwurf sieht lediglich pauschal vor, dass dessen Bestimmungen gemäß § 2 Z 3 SVN-G auf Foren „mit einem größeren Personenkreis anderer Nutzer“ anzuwenden sind, worunter sowohl öffentliche als auch geschlossene Foren fallen können.

²³⁴ *Hengstschläger/Leeb*, Grundrechte³ (2019) 224;
Wessely, Wir werden keinen Richter brauchen... – oder vielleicht doch? Altes und Neues zum Fernmeldegeheimnis, in FS Berka (2013) 277 (287).

erfüllen, als diese abzulehnen.²³⁵ So besteht die ernste Gefahr, dass die Maßnahmen des SVN-G letztendlich zu einem „Overblocking“ führen, also zur Unterbindung von eigentlich rechtskonformen Postings durch die Diensteanbieter.²³⁶ Ein solches Vorgehen würde zu massiven Beeinträchtigungen des Grundrechts auf freie Meinungsäußerung und Informationsfreiheit führen.²³⁷ Die Vorprüfung der Anträge durch ein Gericht oder eine unabhängige Behörde könnte die Gefahr des „Overblocking“ jedoch eindämmen. Im Übrigen wurde auch das eingangs erwähnte französische Gesetz gegen „Hass im Netz“ in erster Linie wegen darin enthaltener zu starker Anreize zum „Overblocking“, die sich in sehr ähnlicher Form auch im SVN-G finden, vom französischen Verfassungsgericht aufgehoben, nämlich vor allem wegen einer zu einseitigen Bußgeldregelung, die lediglich die Nichtbefolgung von Anträgen, nicht aber die Überschreitung der Befugnisse der Diensteanbieter pönalisierte.²³⁸

5.6.7 Technische und organisatorische Maßnahmen zum Schutz der Daten

Um der Verpflichtung des § 1 Abs 2 DSG, „angemessene Garantien für den Schutz der Geheimhaltungsinteressen“²³⁹ der von den Eingriffsmaßnahmen Betroffenen festzulegen, gerecht zu werden, müsste das Gesetz auch technische und organisatorische Maßnahmen zum Schutz der Vorratsdaten vorsehen.²⁴⁰ Derartige Datensicherheitsmaßnahmen fehlen jedoch im SVN-G.

Eine zielführende Schutzmaßnahme wäre etwa der Einsatz von sicheren Verschlüsselungsmethoden. So sollte die Übermittlung von Nutzerdaten im Anwendungsbereich des SVN-G nur in verschlüsselter Form über eine zentrale, elektronische Schnittstelle erfolgen, so wie es bereits bei der Übermittlung von Telekommunikationsdaten (Betriebsdaten) an Strafver-

²³⁵ Vgl. *Wienfort*, Blocking Overblocking. Frankreichs Verfassungsrat kippt das Gesetz gegen Hasskriminalität im Netz, Website Verfassungsblog.de 20.06.2020 <www.verfassungsblog.de/blocking-overblocking> (abgefragt am 14.01.2022).

²³⁶ Vgl. *Berka/Trappel*, Internetfreiheit in Österreich, REM Bd 17 (2019) 60.

²³⁷ *Zankl*, Host-Provider: Löschung rechtswidriger wort- und sinngleicher Postings, *ecolex* 2021/10, 24 (25).

²³⁸ *Wienfort*, Blocking Overblocking. Frankreichs Verfassungsrat kippt das Gesetz gegen Hasskriminalität im Netz, Website Verfassungsblog.de 20.06.2020 <www.verfassungsblog.de/blocking-overblocking> (abgefragt am 14.01.2022).

²³⁹ § 1 Abs 2 DSG.

²⁴⁰ Vgl. VfGH 27.06.2014, G 47/2012 ua, Rz 187 ff.

folgungsbehörden gemäß §§ 102a ff TKG angewendet wird.²⁴¹ Dieses Konzept könnte aufgrund des sehr ähnlichen Regelungsgenstands auch für das SVN-G herangezogen werden. Verkehrs- und Standortdaten im Sinne des TKG werden gemäß §§ 102a ff TKG über die sogenannte Durchlaufstelle, die als speziell gesichertes elektronisches Postfach beim Bundesministerium für Inneres eingerichtet ist, übermittelt.²⁴² Dabei werden sowohl die richterlich genehmigten Anträge auf Übermittlung von Nutzerdaten an die betreffenden Telekomunternehmen, als auch die Ausfolgung der angeforderten Daten durch diese jeweils über die zentrale Schnittstelle abgewickelt. Die Daten werden dabei stets in verschlüsselter Form übermittelt, um unberechtigtem Zugriff vorzubeugen. Die Verantwortung für die Datensicherheit obliegt dabei gemäß § 102c Abs 1 TKG sinnvollerweise dem Bundesministerium für Inneres und nicht etwa den Telekomunternehmen selbst.²⁴³

Im Anwendungsbereich des SVN-G könnten die Ansuchen auf Übermittlung von Nutzerdaten bei einer zentralen Durchlaufstelle zudem einer weiteren Vorprüfung unterzogen und gegebenenfalls in eine bestimmte Form gebracht werden. So könnten sich die Diensteanbieter auf ein einheitliches Format einstellen, was wiederum die Rechtssicherheit fördert. Die Übermittlung der Nutzerdaten durch die Diensteanbieter sollte ebenfalls über eine verschlüsselte Verbindung über die Durchlaufstelle als Zwischenstation erfolgen. Die Durchlaufstelle könnte die Daten dann an die ansuchenden Stellen weiterleiten. Dies würde den Diensteanbietern die Last abnehmen, selbst für die Datensicherheit sorgen zu müssen. Im Ergebnis wäre es so möglich, die Gefahr von Missbrauch und unbefugtem Zugang zu den Daten zu minimieren, wie von den Höchstgerichten für vergleichbare Sachverhalte der Vorratsdatenspeicherung gefordert.²⁴⁴

²⁴¹ §§ 102a bis 102c TKG 2003 idF BGBl I 78/2018, nicht zu verwechseln mit den am 30.06.2014 außer Kraft getretenen Vorgängerbestimmungen zur aufgehobenen Vorratsdatenspeicherung.

²⁴² §§ 102a ff TKG.

²⁴³ § 102c Abs 1 TKG.

²⁴⁴ Vgl VfGH 27.06.2014, G 47/2012 ua, Rz 188; vgl EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 66; vgl EuGH 21.12.2016, C-203/15, C-698/15 (*Tele2 Sverige* und *Watson u.a.*) Rz 122.

5.6.8 Zeitstempel sind nicht verhältnismäßig

Ebenfalls zu hinterfragen, ist die den Diensteanbietern gemäß § 3 Abs 6 Z 3 SVN-G auferlegte Pflicht, periodisch zu überprüfen, ob ein Nutzer regelmäßig im Forum aktiv ist.²⁴⁵ Die zur Bewerkstelligung dieser Überprüfung notwendige Sammlung von Daten in der Form von Zeitstempeln leistet nämlich keinen ersichtlichen Beitrag zur Erreichung der Ziele des SVN-G, weshalb man bereits die Erforderlichkeit dieser Kontrolle anzweifeln könnte. Da eine festgestellte Inaktivität eines Nutzers von mehr als einem Jahr aber die Löschung dessen Registrierungsprofilaten zur Folge hätte,²⁴⁶ könnte man dies auch als grundsätzlich sinnvolle Maßnahme zur Datenminimierung interpretieren. Allerdings muss mit den massenhaft zu speichernden Zeitstempeln eine zusätzliche Datenkategorie geschaffen werden, die direkte und weitreichende Rückschlüsse auf das Surfverhalten und die Lebensgewohnheiten der Nutzer zulässt. Dies stellt einen weiteren Grundrechtseingriff dar, dessen negative Auswirkungen und potentielle Risiken jedoch schwerer wiegen, als der Nutzen, den dieser bezwecken soll. Die Pflicht zur regelmäßigen Überprüfung der Aktivität der Nutzer durch die Speicherung von Zeitstempeln ist daher unverhältnismäßig.

5.6.9 Löschpflichten und zeitlich begrenzte Speicherdauer

Der durch das SVN-G bewirkte Eingriff in das Grundrecht auf Datenschutz muss in angemessener Weise beschränkt sein und darf den zur Zielerreichung erforderlichen Umfang nicht übersteigen. Dazu gehört auch eine Eingrenzung der zulässigen Speicherdauer der Daten auf das absolut notwendige Maß. Zudem muss im Einklang mit der Rechtsprechung zum Grundrecht auf Datenschutz und dem Recht auf Achtung des Privat- und Familienlebens die verpflichtende unwiderrufliche Löschung der Daten vorgesehen sein, die spätestens dann schlagend wird, wenn entweder die höchstzulässigen Speicherfristen erreicht sind oder der Speicherzweck, welcher in der den Eingriff ermöglichenden Rechtsnorm vorgesehen ist, wegfällt.²⁴⁷

²⁴⁵ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 6 Z 3.

²⁴⁶ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 6 Z 3.

²⁴⁷ Vgl VfGH 11.12.2019, G 72-74/2019, G 181-182/2019, Rz 70;

EGMR 04.12.2008, 30562/04 und 30566/04 (GK) (*S. und Marper gg Vereinigtes Königreich*) Z 103; *Berka*, Öffentliches Recht. Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT I/1 (2012) 116.

Das SVN-G sieht zwar konkrete Löschpflichten vor, jedoch nur für das sogenannte Registrierungsprofil, welches Vorname, Nachname und Adresse eines Nutzers umfasst. Demnach müssen diese Registrierungsprofilaten eines Nutzers nur in den in § 3 Abs 6 SVN-G genannten Fällen gelöscht werden, nämlich kurz zusammengefasst, wenn der Nutzer sich von der Nutzung des Forums abmeldet oder er wegen längerer Inaktivität vom Diensteanbieter gesperrt werden muss.²⁴⁸

Dies reicht jedoch nicht aus. So enthält das SVN-G beispielsweise keine Klarstellung, wie mit den Postings eines gelöschten Nutzers umzugehen ist. Der Interpretation des Entwurfs zufolge müssten nämlich auch Aufzeichnungen von Postings von bereits gelöschten Nutzern gemäß § 4 Abs 4 SVN-G angefertigt und an Ansuchende herausgegeben werden und dies offensichtlich sogar zeitlich unbegrenzt.

5.6.10 Speicherung der Nutzerdaten im Unionsgebiet

Das SVN-G enthält außerdem keine Vorgaben, was den Aufbewahrungsort der zu sammelnden personenbezogenen Nutzerdaten anbelangt. Erforderlich wäre jedoch eine Speicherung der Daten innerhalb der Europäischen Union, damit gewährleistet werden kann, dass die Datenverarbeitung unter dem einheitlichen Schutzniveau der DSGVO erfolgt, was zudem auch für die Vermeidung von Datenmissbrauch förderlich wäre.²⁴⁹ Weil das SVN-G keine diesbezüglichen Regeln enthält, wäre eine Speicherung der Nutzerdaten durch die Diensteanbieter auch außerhalb des Unionsgebiets möglich und damit wohl auch in Staaten, die ein deutlich geringeres Schutzniveau aufweisen, als die EU-Mitgliedstaaten.²⁵⁰

²⁴⁸ ME SVN-G, Gesetzestext, 134/ME XXVI. GP, § 3 Abs 6.

²⁴⁹ Vgl EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 68.

²⁵⁰ Der EuGH beanstandet bei der Prüfung der Vorratsdatenspeicherungsrichtlinie im Urteil EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 68 ebenfalls das Fehlen einer verpflichtenden Speicherung von Vorratsdaten innerhalb des Unionsgebiets mit der Begründung, dass nur dadurch der Schutz personenbezogener Daten von einer unabhängigen Stelle überwacht werden kann, wie in Art 8 Abs 3 GRC vorgesehen.

5.6.11 Identifizierungspflicht des SVN-G bewirkt „chilling effects“

Diskussionsforen im Internet bieten den Nutzern eine Plattform für den ungezwungenen Austausch zu allen erdenklichen, oft frei wählbaren Themen. Sie dienen somit ausschließlich dem Zweck der Ausübung des Grundrechts auf freie Meinungsäußerung und Informationsfreiheit. Die ganz überwiegende Mehrheit der Nutzer verwendet Onlineforen auch allein in der Absicht, mit anderen Leuten zu diskutieren und damit von diesem verfassungsgesetzlich gewährleisteten Recht Gebrauch zu machen - und nicht etwa mit der Intention, im Forum rechtswidrige Äußerungen zu tätigen.²⁵¹ Damit ist schon jede Berührung der Ausübung dieses Grundrechts als problematisch zu sehen.²⁵²

Eine Identifizierungspflicht sämtlicher Nutzer, wie sie das SVN-G vorsieht, stellt eine Zugangsbarriere zu Diskussionsforen und damit auch zur Ausübung des Grundrechts auf freie Meinungsäußerung dar. Die Nutzer werden damit, bereits bevor sie in einem Forum ihr Meinung überhaupt kundtun können, im Zuge der Registrierung ihrer persönlichen Daten unsanft daran erinnert, dass die Staatsgewalt ein Auge auf ihre Äußerungen im Forum wirft. Dies kann dazu führen, dass in Bürgern, die vom SVN-G betroffene Diskussionsforen nutzen möchten, das Gefühl entsteht, dass ihr Privatleben einer permanenten staatlichen Überwachung unterliegt.²⁵³

Deshalb ist davon auszugehen, dass diese Registrierungs- und Identifizierungspflicht sowie die Verarbeitung und Ausfolgung der vom SVN-G umfassten Kategorien personenbezogener Daten nachteilige Auswirkungen auf die Akzeptanz der betroffenen Foren zur Folge hätten. Da die zu speichernden Daten deutliche Schlüsse auf das Privatleben der Nutzer zulassen würden, muss damit gerechnet werden, dass die Maßnahmen des SVN-G sich durch stark sinkendes Interesse an der Kommunikation in Internetforen bemerkbar machen würden. Der EuGH gelangte in den Urteilen *Digital Rights Ireland* und *Tele2 Sverige* zu ebendieser Ansicht wonach eine anlasslose Vorratsdatenspeicherung zu einer verminderten Nutzung der betroffenen Kommunikationsmittel führt und dies trotz des Um-

²⁵¹ Vgl VfGH 27.06.2014, G 47/2012 ua, Rz 183.

²⁵² Vgl *Hengstschläger/Leeb*, Grundrechte³ (2019) 247; siehe dazu auch *Bezemek*, Freie Meinungsäußerung. Fragen des Grundrechtseingriffs, Fragen der Grundrechtsausübung, ZÖR 2012, 557 (560 ff).

²⁵³ Vgl GA 12.12.2013, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 52 u 72; vgl EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 37; vgl EuGH 21.12.2016, C-203/15, C-698/15 (*Tele2 Sverige* und *Watson u.a.*) Rz 100.

stands, dass die Kommunikationsinhalte von der dort gegenständlichen Vorratsspeicherung von Telekommunikationsdaten gar nicht umfasst waren.²⁵⁴

Im Fall des SVN-G sind aber mit der verpflichtenden Anfertigung und Herausgabe von Aufzeichnungen der Postinginhalte nun sehr wohl auch die Inhalte der Kommunikation zu verarbeiten und gegenüber den Antragstellern offenzulegen. Wo dies der EuGH selbst bei Nichtbetroffenheit des Kommunikationsinhalts bereits erwartet hat, so ist es im Fall des SVN-G daher noch um einiges wahrscheinlicher, dass viele Bürger von der Nutzung der Diskussionsforen und damit der Ausübung ihrer freien Meinungsäußerung im Internet vermehrt Abstand nehmen würden. Abgesehen von der Betroffenheit der Postinginhalte ist davon auszugehen, dass bereits allein die vom SVN-G aufgezwungene Überprüfung und Speicherung des Namens und der Adresse eines jeden Nutzers abschreckende Wirkung zeigen und zu sinkenden Nutzerzahlen und damit zu einer deutlich verringerten Akzeptanz der Foren durch die Bürger führen würde. Hier spielt aber weniger die Befürchtung eine Rolle, als Forennutzer möglicherweise unverschuldet strafrechtlichen Ermittlungen ausgesetzt werden zu können, sondern vielmehr die Tatsache, dass aufgrund der beim Diensteanbieter zu speichernden Personalien stets die Identität eines jeden Nutzers aufgedeckt werden könnte. Einschüchternd kann bereits der Umstand wirken, dass einzelne Mitarbeiter des Diensteanbieters theoretisch jederzeit Name und Adresse eines Posters in der Datenbank nachschlagen könnten. Auch die Gefahr, dass es zu einem unberechtigten Zugriff von außen oder gar zu einem Diebstahl der Nutzerdaten kommen könnte, darf nicht übersehen werden. Dieses Risiko hat sich im Fall der mittlerweile wieder aufgehobenen Klarnamenpflicht in Südkorea tatsächlich verwirklicht, wo es zu mehreren großangelegten Diebstählen der Identitätsdaten von Millionen Bürgern gekommen ist.²⁵⁵

Es gibt Dinge, die man ungern öffentlich preisgibt. Sei es Kritik an Politik und Institutionen, dem Arbeitgeber, Informationen zur körperlichen und geistigen Gesundheit oder kontroverse persönliche Ansichten zu gesellschaftlichen Fragen, um einige Beispiele zu nennen. Aber gerade die Anonymität von Diskussionsplattformen im Internet bietet die Sicherheit, sich über solche Themen in einem geschützten Rahmen austauschen zu können. Fraglich ist, inwiefern die Bürger noch dazu bereit wären, diesen Diskurs in Internetforen zu führen, wenn die Anonymität fallen und zumindest der Diensteanbieter ihren Namen

²⁵⁴ EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 27 f;
EuGH 21.12.2016, C-203/15, C-698/15 (*Tele2 Sverige* und *Watson u.a.*) Rz 101.

²⁵⁵ *Brodnig*, Der unsichtbare Mensch. Wie die Anonymität im Internet unsere Gesellschaft verändert (2013) 145 f.

und ihre Adresse kennen würde. Letztendlich ist davon auszugehen, dass eine Identifizierungspflicht wie das SVN-G nicht nur potentielle Hassposter abschrecken, sondern in weit größerem Umfang dazu führen würde, dass auch zahlreiche seriöse Nutzer, die Wert auf Vertraulichkeit und Schutz ihrer Privatsphäre legen, den Foren fernbleiben würden. Im Ergebnis würde dadurch die Diskussionsbereitschaft im Netz stetig sinken und die Qualität des Diskurses zunehmend verflachen.

Solche unerwünschten abschreckenden Auswirkungen von in das Grundrecht auf Meinungsfreiheit eingreifenden Maßnahmen, die dazu führen, dass die Bürger zunehmend davon Abstand nehmen, von ihrem Recht auf freie Meinungsäußerung Gebrauch zu machen, nennt man auch „chilling effects“.²⁵⁶

5.7 Ergebnis der Grundrechtsprüfung

Zusammenfassend betrachtet steht damit fest, dass die Maßnahmen des SVN-G intensive Einschränkungen des Grundrechts auf Datenschutz und des Rechts auf Achtung des Privat- und Familienlebens der Nutzer der betroffenen Diskussionsforen verursachen. Darüber hinaus bewirkt das SVN-G einen schwerwiegenden Eingriff in das Grundrecht auf freie Meinungsäußerung und Informationsfreiheit.

Zudem weist das SVN-G in zahlreichen Details gravierende Mängel auf, was auch dazu führt, dass es den Eingriffsermächtigungen in das Grundrecht auf Datenschutz und das Grundrecht auf Achtung des Privat- und Familienlebens an der erforderlichen ausreichenden Bestimmtheit mangelt.²⁵⁷ Das SVN-G unterlässt es dadurch in vielen Fällen, für die gebotene Verhältnismäßigkeit der ermöglichten Eingriffe zu sorgen, da es die im grundlegenden Erkenntnis des VfGH zur Vorratsdatenspeicherung geforderten spezifischen Garantien beinahe vollständig vermissen lässt.²⁵⁸

²⁵⁶ *Mersch*, Die Kommunikationsfreiheit im Lichte der VfGH-Judikatur, JAP 2015/2016/13, 139 (141); *Bezemek*, Freie Meinungsäußerung. Fragen des Grundrechtseingriffs, Fragen der Grundrechtsausübung, ZÖR 2012, 557 (559 f); *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention⁷ (2021) 418 Rz 29.

²⁵⁷ *Berka*, Öffentliches Recht. Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT I/1 (2012) 115 f; *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention⁷ (2021) 319 Rz 39 ff.

²⁵⁸ Vgl VfGH 27.06.2014, G 47/2012 ua, Rz 168.

Die in der Prüfung bereits ausführlich dargestellten, ausschlaggebenden Unzulänglichkeiten des SVN-G lassen sich in den folgenden Kategorien noch einmal kurz zusammenfassen:

Maßnahmen sind nur zur Verfolgung schwerer Straftaten zulässig

So fehlt in erster Linie eine notwendige Eingrenzung des Anwendungsbereichs des SVN-G auf bestimmte, schwere Straftaten.²⁵⁹ Auch eine Beschränkung auf Straftatbestände, die typischerweise mit der Verbreitung von Hasspostings in Zusammenhang stehen, liegt nicht vor. Vielmehr könnte das SVN-G zur Verfolgung jeder erdenklichen Straftat und damit auch bereits leichtester Delikte herangezogen werden.²⁶⁰

Betroffener Personenkreis zu weit gefasst

Zudem weist das SVN-G eine enorm große „Streubreite“ auf, es fehlt eine angemessene Einschränkung auf einen engeren Personenkreis. Stattdessen sind praktisch alle Nutzer der umfassten Onlinedienste und damit ein großer Teil der Bevölkerung ausnahmslos betroffen, wobei davon auszugehen ist, dass der ganz überwiegende Anteil der betroffenen Bürger bei der Nutzung von Diskussionsforen zu keiner Zeit einen Anlass begründen wird, um Strafverfolgungsmaßnahmen wie jene des SVN-G anzuwenden.²⁶¹

Gefahr des Missbrauchs und des unbefugten Zugriffs auf die Nutzerdaten

Der Entwurf enthält keine Vorkehrungen zum Schutz vor Missbrauch der auf Vorrat gesammelten personenbezogenen Daten, die Rückschlüsse auf den höchstpersönlichen Lebensbereich der Nutzer enthalten und unter anderem deshalb einen erheblichen wirtschaftlichen Wert verkörpern. Durch die Vielzahl von speicherungsverpflichteten Diensteanbietern steigt auch die Missbrauchsgefahr, beispielsweise durch unbefugten Zugriff auf die Daten.²⁶²

²⁵⁹ Vgl VfGH 27.06.2014, G 47/2012 ua, Rz 171;
vgl EuGH 21.12.2016, C-203/15, C-698/15 (*Tele2 Sverige und Watson u.a.*) Rz 115.

²⁶⁰ Vgl VfGH 11.12.2019, G 72-74/2019, G 181-182/2019, Rz 103 ff.

²⁶¹ Vgl VfGH 27.06.2014, G 47/2012 ua, Rz 183 f;
vgl EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland und Seitlinger u.a.*) Rz 58.

²⁶² Vgl VfGH 27.06.2014, G 47/2012 ua, Rz 187.

Materiell- und verfahrensrechtliche Regeln für den Zugang zu den Nutzerdaten

Des Weiteren fehlen präzise materiell- und verfahrensrechtliche Bestimmungen, die den Zugang zu den Nutzerdaten regeln und vorgeben, auf welche Weise die Übermittlung der Daten zu erfolgen hat.²⁶³ Außerdem werden die betroffenen Nutzer nicht informiert, wenn der Diensteanbieter ihre gespeicherten personenbezogenen Daten herausgibt. Dadurch wird den Nutzern die Möglichkeit vorenthalten, zeitgerecht Rechtsmittel gegen die Maßnahmen einzuwenden. Eigenständige Rechtsmittel für betroffene Nutzer fehlen im Entwurf.²⁶⁴

Vorprüfung und Kontrolle durch Gericht oder unabhängige Behörde

Das SVN-G müsste vorsehen, dass Ansuchen auf Übermittlung von Nutzerdaten einer Vorprüfung und Kontrolle durch ein Gericht oder eine unabhängige Behörde unterworfen werden.²⁶⁵ So könnte auch verhindert werden, dass Diensteanbieter Daten herausgeben, obwohl die rechtlichen Voraussetzungen dazu nicht vorliegen.

Gefahr des „Overblocking“

Zudem könnte durch Vorprüfung und Kontrolle durch ein Gericht oder eine unabhängige Behörde auch die Gefahr minimiert werden, dass es zu einem „Overblocking“ kommt, also der Beanstandung und Unterbindung von grundsätzlich rechtskonformen Postings durch die Diensteanbieter,²⁶⁶ was wiederum eine Beeinträchtigung der Meinungsfreiheit zur Folge hätte.²⁶⁷

Technische und organisatorische Maßnahmen zum Schutz der Daten

Außerdem lässt der Entwurf technische und organisatorische Maßnahmen zum Schutz der Daten vermissen.²⁶⁸ Entsprechend dem vergleichbaren Fall der Übermittlung von Telekommunikationsdaten an Strafverfolgungsbehörden müsste eine verschlüsselte und

²⁶³ EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 61.

²⁶⁴ Vgl VfGH 11.12.2019, G 72-74/2019, G 181-182/2019, Rz 105;
vgl EuGH 21.12.2016, C-203/15, C-698/15 (*Tele2 Sverige* und *Watson u.a.*) Rz 121.

²⁶⁵ Vgl EuGH 21.12.2016, C-203/15, C-698/15 (*Tele2 Sverige* und *Watson u.a.*) Rz 120;
vgl VfGH 27.06.2014, G 47/2012 ua, Rz 168 u 175;
vgl VfGH 11.12.2019, G 72-74/2019, G 181-182/2019, Rz 105.

²⁶⁶ Vgl *Berka/Trappel*, Internetfreiheit in Österreich, REM Bd 17 (2019) 60.

²⁶⁷ *Zankl*, Host-Provider: Löschung rechtswidriger wort- und sinngleicher Postings, *ecolex* 2021/10, 24 (25).

²⁶⁸ Vgl VfGH 27.06.2014, G 47/2012 ua, Rz 187 ff.

standardisierte Datenübermittlung über eine Durchlaufstelle als Schnittstelle zu den ansuchenden Stellen sichergestellt werden.

Zeitstempel sind nicht verhältnismäßig

Die Pflicht zur regelmäßigen Überprüfung der Aktivität der Nutzer durch die Speicherung von Zeitstempeln ist unverhältnismäßig, da die negativen Auswirkungen und potentiellen Risiken des dadurch verursachten Grundrechtseingriffs schwerer wiegen, als der Nutzen, den diese Überprüfungspflicht bezwecken soll.

Löschpflichten und zeitlich begrenzte Speicherdauer

Das SVN-G sieht teilweise weder eine auf den Zweck der Eingriffsmaßnahmen begrenzte Speicherdauer noch Löschpflichten betreffend bestimmte Daten vor.²⁶⁹

Speicherung der Nutzerdaten im Unionsgebiet

Das SVN-G gibt nicht vor, wo die Nutzerdaten gespeichert werden müssen. Eine verpflichtende Speicherung der personenbezogenen Daten im Unionsgebiet wäre jedoch erforderlich, damit gewährleistet werden kann, dass die in § 1 DSG enthaltenen Vorschriften bezüglich des Schutzes von personenbezogenen Daten eingehalten werden.²⁷⁰

Identifizierungspflicht des SVN-G bewirkt „chilling effects“

Als besonders schwerwiegend erweisen sich die Eingriffe des SVN-G in das Grundrecht auf Meinungs- und Informationsfreiheit. Die Pflicht zur lückenlosen Identifizierung sämtlicher Personen, die daran interessiert sind, betroffene Onlinedienste zu nutzen, und die Speicherung der gesammelten personenbezogenen Daten auf Vorrat für spätere Strafverfolgungsmaßnahmen würde viele Bürger von der Nutzung der betroffenen Diskussionsplattformen abschrecken. Diese „chilling effects“ und die damit verbundene Gefahr, dass sich ein Gefühl der permanenten Überwachung des Privatlebens einstellt,²⁷¹

²⁶⁹ Vgl VfGH 11.12.2019, G 72-74/2019, G 181-182/2019, Rz 70; EGMR 04.12.2008, 30562/04 und 30566/04 (GK) (*S. und Marper gg Vereinigtes Königreich*) Z 103; *Berka*, Öffentliches Recht. Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT I/1 (2012) 116.

²⁷⁰ Vgl EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 68.

²⁷¹ Vgl GA 12.12.2013, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 52 u 72; vgl EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 37; vgl EuGH 21.12.2016, C-203/15, C-698/15 (*Tele2 Sverige* und *Watson u.a.*) Rz 100.

würden zu einer stark verringerten Diskussionsbereitschaft im Internet und damit zu einer verminderten Ausübung des Grundrechts auf freie Meinungsäußerung durch die Bürger führen.²⁷²

Somit gelangt man zum Ergebnis, dass das mit dem SVN-G angestrebte Ziel, die Verfolgung von durch Hasspostings verursachten Straftaten und Rechtsansprüchen zu erleichtern, zwar grundsätzlich im öffentlichen Interessen liegen mag, aber dennoch die durch die einzelnen Maßnahmen des Gesetzesentwurfs ermöglichten Grundrechtseingriffe wesentlich schwerer wiegen. Da die Eingriffe sämtliche Nutzer der betroffenen Diskussionsplattformen ausnahmslos erfassen, bewirkt dies die systematische Kontrolle eines gesamten, ausschließlich der freien Meinungsäußerung dienenden Kommunikationsbereichs.²⁷³ Dadurch werden wichtige Möglichkeiten der unbeeinflussten Meinungsbildung und der freien, zwischenmenschlichen Kommunikation und damit auch fundamentale Werte einer demokratischen Gesellschaft gefährdet.²⁷⁴

Angesichts der zahlreichen Mängel des Entwurfs wird deutlich, dass die ermöglichten Eingriffe sich keinesfalls auf das absolut notwendige Mindestmaß beschränken und die konkreten Maßnahmen des SVN-G, welche die umfangreichen Eingriffe in das Datenschutzgrundrecht und das Grundrecht auf Achtung des Privat- und Familienlebens der Betroffenen bewirken, auch nicht die gelindesten zur Verfügung stehenden Mittel darstellen. Darüber hinaus fehlen dem SVN-G hinreichend präzise und für jedermann vorhersehbare Bestimmungen, die die Zulässigkeit der Ermittlung und der Verwendung der personenbezogenen Nutzerdaten regeln.²⁷⁵

²⁷² Vgl. EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 27 f; vgl. EuGH 21.12.2016, C-203/15, C-698/15 (*Tele2 Sverige* und *Watson u.a.*) Rz 101; *Mersch*, Die Kommunikationsfreiheit im Lichte der VfGH-Judikatur, JAP 2015/2016/13, 139 (141); *Bezemek*, Freie Meinungsäußerung. Fragen des Grundrechtseingriffs, Fragen der Grundrechtsausübung, ZÖR 2012, 557 (559 f); *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention⁷ (2021) 418 Rz 29.

²⁷³ Vgl. *Berka*, Öffentliches Recht. Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT I/1 (2012) 78.

²⁷⁴ Vgl. *Berka*, Öffentliches Recht. Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT I/1 (2012) 78.

²⁷⁵ Vgl. *Berka*, Öffentliches Recht. Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT I/1 (2012) 115 f; *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention⁷ (2021) 318 Rz 38 ff.

Besonders schwer wiegen die durch die Maßnahmen des SVN-G verursachten Beeinträchtigungen des Grundrechts auf freie Meinungsäußerung. Dies manifestiert sich einerseits in der ernststen Gefahr, dass die Bestimmungen des SVN-G, insbesondere die einseitigen und hohen Bußgelder, die Diensteanbieter zum „Overblocking“ verleiten könnten, also der Unterdrückung von rechtmäßigen Meinungsäußerungen der Nutzer. Zudem resultieren die Maßnahmen in „chilling effects“, was als absehbare Folge unweigerlich zur verminderten Nutzung der betroffenen Diskussionsplattformen führen würde.²⁷⁶

Im Ergebnis steht damit fest, dass die Summe dieser Mängel bewirkt, dass die Maßnahmen des SVN-G, die diese schweren Grundrechtseingriffe ermöglichen und herbeiführen, insgesamt als nicht verhältnismäßig zu qualifizieren sind und daher Verletzungen der angeführten Grundrechte verursachen. Das SVN-G ließe sich in der gegenständlichen Form daher in Österreich nicht grundrechts- und verfassungskonform umsetzen.

²⁷⁶ Vgl. EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland* und *Seitlinger u.a.*) Rz 27 f; vgl. EuGH 21.12.2016, C-203/15, C-698/15 (*Tele2 Sverige* und *Watson u.a.*) Rz 101.

6. Conclusio - Eignung von Identifizierungs- und Klarnamenpflichten zur Bekämpfung von „Hass im Netz“

Selbst wenn es gelingen würde, viele der aufgezeigten Mängel des Gesetzesentwurfs zu beheben und das SVN-G zumindest betreffend die Eingriffe in das Datenschutzgrundrecht und das Grundrecht auf Achtung des Privat- und Familienlebens tatsächlich verhältnismäßig auszugestalten, so würde am Ende dennoch das grundlegende Problem des schweren und unverhältnismäßigen Eingriffs in das Grundrecht auf freie Meinungsäußerung und Informationsfreiheit bestehen bleiben, das sich insbesondere in „chilling effects“ in Form des Vertrauensverlusts der Bürger in die betroffenen Diskussionsplattformen niederschlägt.

Demokratische Gesellschaften garantieren ihren Bürgern typischerweise die Sicherheit, ihre Meinung jederzeit unbeeinflusst äußern zu können. Selbstverständlich muss die freie Meinungsäußerung dabei immer auch gewissen rechtlichen Grenzen unterliegen, was sich darin zeigt, dass Äußerungen beim Verdacht einer Rechtsverletzung gegebenenfalls einer rechtlichen Beurteilung unterzogen werden können. Falls dies tatsächlich nötig sein sollte, erfolgt dies jedoch stets nachträglich, es wird keinem Bürger von vornherein das Wort verboten.

Im Gegensatz dazu verfolgen Klarnamenpflichten und Identifizierungspflichten wie das SVN-G jedoch einen etwas anderen Ansatz. So wirken diese in gewisser Weise bereits ex ante, indem sie Personen, die beabsichtigen, im Internet ihre persönliche Meinung zu äußern, durch den Identifizierungszwang schon vorsorglich die Rute ins Fenster stellen. Durch die Überprüfung und Speicherung ihrer Identitätsdaten wird den Bürgern nämlich vor Augen geführt, dass ihr Kommunikationsverhalten im Netz stets einer staatlichen Kontrolle unterliegt. Mit der Einführung einer Identifizierungspflicht würde der Gesetzgeber somit zu verstehen geben, dass er jedem Forennutzer prinzipiell zutraut, rechtswidrige Äußerungen im Netz zu tätigen, was beinahe einem Generalverdacht gleichkäme. Es liegt auf der Hand, dass als Folge dessen die Bereitschaft der Bürger, ihre Meinung im Internet zu äußern, dramatisch sinken würde.

Solche negativen, abschreckenden Begleiterscheinungen sind jedoch keine Besonderheit, die nur beim Entwurf des SVN-G auftreten. Vielmehr haften derartige „chilling effects“ Identifizierungs- und Klarnamenpflichten generell bereits von Grund auf an, da diese stets die dafür ursächlichen Maßnahmen enthalten müssten: die anlasslose Überprüfung und Speicherung der Identitätsdaten sämtlicher Nutzer auf Vorrat. Diese Maßnahmen müssten

in jedem Fall durchgeführt werden, bei der Variante einer Klarnamenpflicht müssten die Identitätsdaten zudem sogar öffentlich sichtbar gemacht werden.

Es ist daher praktisch keine Variante einer Identifizierungs- oder Klarnamenpflicht denkbar, die nicht in „chilling effects“ und somit letztendlich in einer Verletzung des Grundrechts auf freie Meinungsäußerung resultieren würde.

Damit steht fest, dass sich Identifizierungs- und Klarnamenpflichten nicht als geeignete Mittel erweisen, um „Hass im Netz“ effektiv entgegenzuwirken. Der Preis, den die Gesellschaft aufgrund der zu erwartenden unverhältnismäßigen Beeinträchtigung und verminderten Ausübung des Rechts auf freie Meinungsäußerung durch den absehbaren Vertrauensverlust der Bürger in die betroffenen Kommunikationsplattformen zu zahlen hätte, wäre zu hoch und würde den Erwartungen an einen demokratischen Rechtsstaat, der dieses elementare Grundrecht stets zu schützen hat, nicht gerecht werden.

7. Literaturverzeichnis

Beiträge in Fachzeitschriften, Festschriften, Sammelwerken und Kommentaren sowie Monografien

Anderl, Axel, Kein Auskunftsanspruch bei dynamischer IP-Adresse, *ecolex* 2012/367, 904

Bergauer, Christian / Jahnel, Dietmar (Hrsg), DSGVO und DSG. Das neue Datenschutzrecht³ (Jan Sramek, Wien 2018)

Berka, Walter / Trappel, Josef, Internetfreiheit in Österreich, Bd 17 der Schriftenreihe Recht der elektronischen Massenmedien REM (Manz, Wien 2019)

Berka, Walter, Öffentliches Recht. Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, 18. ÖJT I/1 (Manz, Wien 2012)

Bezemek, Christoph, Freie Meinungsäußerung. Fragen des Grundrechtseingriffs, Fragen der Grundrechtsausübung, *ZÖR* 2012, 557

Bezemek, Christoph in Holoubek/Lienbacher (Hrsg), Charta der Grundrechte der Europäischen Union. GRC-Kommentar² (Manz, Wien 2019) Art 11

Brodnig, Ingrid, Der unsichtbare Mensch. Wie die Anonymität im Internet unsere Gesellschaft verändert (Czernin, Wien 2013)

Brodnig, Ingrid, Hass im Netz. Was wir gegen Hetze, Mobbing und Lügen tun können (Brandstätter, Wien 2016)

Burger, Christian, Sch(m)utz im Netz. Warum wir digitale Masken brauchen (Leykam, Graz, Wien 2021)

Fötschl, Andreas, Die Entscheidung Delfi des EGMR: Der Einfluss der Grundrechte auf das Host-Provider-Haftungsprivileg, *ecolex* 2015, 827

Grabenwarter, Christoph / Pabel, Katharina, Europäische Menschenrechtskonvention⁷
(C. H. Beck, München 2021)

Haidinger, Viktoria in Knyrim (Hrsg), Der DatKomm. Praxiskommentar zum
Datenschutzrecht - DSGVO und DSG, Art 17 DSGVO (Stand 01.10.2018, rdb.at)

Hengstschläger, Johannes / Leeb, David, Grundrechte³ (Manz, Wien 2019)

Hödl, Elisabeth in Knyrim (Hrsg), Der DatKomm. Praxiskommentar zum
Datenschutzrecht - DSGVO und DSG, Art 4 DSGVO (Stand 01.12.2018, rdb.at)

Jahnel, Dietmar, Handbuch Datenschutzrecht (Jan Sramek, Wien 2010)

Koukal, Alexander, Kritische Äußerungen auf einem Onlineforum als Datenverwendung
iS des DSG - personenbezogene Daten - Untersagung - Widerspruch (§ 28 Abs 2 DSG),
MR 2009, 306

Lehofer, Hans Peter, Hass im Netz und gedruckt: europäische Gerichte, österreichische
Fälle, ÖJZ 2019/112, 893

Mayer, Heinz / Kucsko-Stadlmayer, Gabriele / Stöger, Karl, Grundriss des
österreichischen Bundesverfassungsrechts¹¹ (Manz, Wien 2015)

Mersch, Christopher, Mediengesetzliche Eckpunkte für den Bürgerjournalismus, in
Berka/Holoubek/Leitl-Staudinger (Hrsg), BürgerInnen im Web, Bd 14 der Schriftenreihe
Recht der elektronischen Massenmedien REM (Manz, Wien 2016)

Mersch, Christopher, Die Kommunikationsfreiheit im Lichte der VfGH-Judikatur,
JAP 2015/2016/13, 139

Öhlinger, Theo / Eberhard, Harald, Verfassungsrecht¹² (Facultas, Wien 2019)

Pavlidis, Laura in Holoubek/Lienbacher (Hrsg), Charta der Grundrechte der Europäischen Union. GRC-Kommentar² (Manz, Wien 2019) Art 7

Rami, Michael in Höpfel/Ratz (Hrsg), Wiener Kommentar zum StGB² Vor §§ 111–117 (Stand 01.04.2021, rdb.at)

Reindl-Krauskopf, Susanne / Salimi, Farsam / Stricker, Martin, IT-Strafrecht (Stand 01.09.2018, rdb.at)

Reischauer, Rudolf in Rummel (Hrsg), ABGB³ § 1330 ABGB (Stand 01.01.2004, rdb.at)

Riesz, Thomas in Riesz/Schilchegger (Hrsg), TKG. Telekommunikationsgesetz. Kommentar (Verlag Österreich, Wien 2016) § 92

Riesz, Thomas in Holoubek/Lienbacher (Hrsg), Charta der Grundrechte der Europäischen Union. GRC-Kommentar² (Manz, Wien 2019) Art 8

Rumler-Korinek, Elisabeth / Vranes, Erich in Holoubek/Lienbacher (Hrsg), Charta der Grundrechte der Europäischen Union. GRC-Kommentar² (Manz, Wien 2019) Art 52

Thiele, Clemens, DSB: Medienprivileg für Online-Forum und Postings, jusIT 2018/87, 250

Thiele, Clemens, EuGH: Grenzen des Medienprivilegs für den Bürgerjournalismus, jusIT 2019/27, 82

Wessely, Wolfgang, Wir werden keinen Richter brauchen... – oder vielleicht doch? Altes und Neues zum Fernmeldegeheimnis, in FS Berka (Jan Sramek, Wien 2013) 277

Windhager, Maria / Forgó, Nikolaus, Hasspostings. Bedarf es einer gesetzlichen Verschärfung? AnwBl 2017/98, 592

Wittmann, Heinz / Zöchbauer, Peter, Zum Entwurf eines Bundesgesetzes über Sorgfalt und Verantwortung im Netz. Ein kritischer Überblick, MR 2019, 103

Zankl, Wolfgang, E-Commerce-Gesetz. Kommentar² (Verlag Österreich, Wien 2016)

Zankl, Wolfgang, Host-Provider: Löschung rechtswidriger wort- und sinngleicher Postings, *ecolex* 2021/10, 24

Zankl, Wolfgang / Knaipp, Florian, Neues IT-Recht, *ecolex* 2021/73, 106

Artikel in Blogs und Online-Ausgaben von Zeitungen und Zeitschriften

Al-Youssef, Muzayen, Minister Blümels ominöse Software zur De-Anonymisierung, Website Der Standard 12.04.2019 <www.derstandard.at/2000101256631/Minister-Bluemels-ominoese-Software-zur-De-Anonymisierung> (abgefragt am 14.01.2022)

Al-Youssef, Muzayen, Regierung will Anonymität im Netz abschaffen – mit hohen Strafen, Website Der Standard 10.04.2019
<www.derstandard.at/story/2000101143621/regierung-will-anonymitaet-im-netz-abschaffen-mit-hohen-strafen> (abgefragt am 14.01.2022)

Al-Youssef, Muzayen, Verfassungsgerichtshof hinterfragt Überwachungspaket, Website Der Standard 25.06.2019 <www.derstandard.at/story/2000105396116/bundestrojaner-und-autobahnueberwachung-vor-dem-vfgh> (abgefragt am 14.01.2022)

Brodnig, Ingrid, FPÖ im Internet: Tag für Tag ein Propagandastück, Website Profil 24.05.2016 <www.profil.at/oesterreich/fpoe-strache-internet-tag-tag-propagandastueck-6378335> (abgefragt am 14.01.2022)

Grimm, Oliver, Neues EU-Gesetz könnte Hass im Netz mindern, Website Die Presse 15.01.2021 <www.diepresse.com/5922905/neues-eu-gesetz-konnte-hass-im-netz-mindern> (abgefragt am 14.01.2022)

Hametner, Markus / Mayrhofer, Michael / Müller, Monika / Zirnig, Dieter, Wenn die Post Partei ergreift, Website Addendum 07.01.2019
<www.addendum.org/datenhandel/parteiaffinitaet> (abgefragt am 14.01.2022)

Kotynek, Martin, Gegen Hass im Netz sind Klarnamen keine Lösung, Website Der Standard 04.01.2019 <www.derstandard.at/story/2000095399328/klarnamen-sind-keine-oesung> (abgefragt am 14.01.2022)

Kühl, Eike, Mehr Überwachung ist verständlich – und trotzdem falsch, Website Zeit Online 17.11.2015 <www.zeit.de/digital/datenschutz/2015-11/vorratsdatenspeicherung-ueberwachung-paris-anschlag-terrorismus> (abgefragt am 14.01.2022)

Lang, Rahel, Rassist:innen kommentieren mit identifizierbaren Accounts, Website netzpolitik.org 12.08.2021 <www.netzpolitik.org/2021/anonymitaet-im-netz-rassistinnen-kommentieren-mit-identifizierbaren-accounts> (abgefragt am 14.01.2022)

Lohninger, Thomas, Das Mitmach-Internet in Gefahr: Bundesregierung will Ausweiszwang im Internet einführen, Website Epicenter.Works 10.04.2019
<www.epicenter.works/content/das-mitmach-internet-in-gefahr-bundesregierung-will-ausweiszwang-im-internet-einfuehren> (abgefragt am 14.01.2022)

Löwenstein, Stephan, Der Hass, das Netz und der Tod, Website Frankfurter Allgemeine Zeitung 04.07.2021 <www.faz.net/aktuell/politik/der-hass-das-netz-und-der-tod-17418839> (abgefragt am 14.01.2022)

Mutschler, Stefan / Schmitz, Peter, So funktioniert Mobile Connect, Website Security Insider.de 30.03.2018 <www.security-insider.de/so-funktioniert-mobile-connect-a-700580> (abgefragt am 14.01.2022)

Neuerer, Dietmar, Schäuble fordert Klarnamenpflicht im Netz, Website Handelsblatt 13.01.2020 <www.handelsblatt.com/politik/deutschland/hass-im-internet-schaeuble-fordert-klarnamenpflicht-im-netz/25424450.html?ticket=ST-308700-cAmVkaJJcOapHSJd9SmD-ap6> (abgefragt am 14.01.2022)

Roth, Philipp, Offizielle Facebook Nutzerzahlen für Deutschland (Stand: März 2019), Website allfacebook.de 19.03.2019 <www.allfacebook.de/zahlen_fakten/offiziell-facebook-nutzerzahlen-deutschland> (abgefragt am 14.01.2022)

Silber, Christoph, Facebook muss Straches "Lügen"-Posting zu Armin Wolf in Österreich löschen, Website Kurier 04.05.2020 <www.kurier.at/kultur/medien/facebook-muss-straches-luegen-posting-zu-armin-wolf-in-oesterreich-loeschen/400831475> (abgefragt am 14.01.2022)

Steinke, Ronen, Wer Klarnamen im Netz fordert, hat Bürgerrechte nicht verstanden, Website Süddeutsche Zeitung 12.06.2019 <www.sueddeutsche.de/digital/social-media-klarnamenpflicht-union-internet-1.4482238> (abgefragt am 14.01.2022)

Wienfort, Nora, Blocking Overblocking. Frankreichs Verfassungsrat kippt das Gesetz gegen Hasskriminalität im Netz, Website Verfassungsblog.de 20.06.2020 <www.verfassungsblog.de/blocking-overblocking> (abgefragt am 14.01.2022)

Wimmer, Barbara, Studie: Klarnamen verhindern keine Hasspostings, Website Futurezone 13.01.2021 <futurezone.at/science/studie-klarnamen-verhindern-keine-hasspostings/211.959.224> (abgefragt am 14.01.2022)

Weitere Internetquellen und Artikel ohne Autorennennung

blog.twitter.com, Website 19.02.2021, No room for racist behaviour on Twitter <blog.twitter.com/en_gb/topics/company/2020/no-room-for-racist-behaviour-on-twitter-> (abgefragt am 14.01.2022)

Der Standard, Website 12.11.2020, Oberster Gerichtshof: Facebook muss Hassposting gegen Glawischnig weltweit löschen <www.derstandard.at/story/2000121648569/oberster-gerichtshof-verfuegt-facebook-muss-hassposting-gegen-glawischnig-weltweit-loeschen> (abgefragt am 14.01.2022)

Der Standard, Website 10.05.2019, Digitale Ausweispflicht: Gesetz stößt auf Skepsis bei Experten <www.derstandard.at/story/2000102900226/digitaler-ausweiszwang-gesetz-stoesst-auf-skepsis-bei-experten> (abgefragt am 14.01.2022)

Der Standard, Website 04.01.2019, Dem Hass im Netz keine Chance: Wie DER STANDARD sein Forum moderiert <www.derstandard.at/story/2000095396987/dem-hass-keine-chance-wie-der-standard-sein-forum-moderiert> (abgefragt am 14.01.2022)

Der Standard, Website 25.11.2016, Verhetzung: Fast wöchentlich Prozesse gegen Hassposter <www.derstandard.at/story/2000048178327/verhetzung-fast-woechentlich-prozesse-gegen-hassposter> (abgefragt am 14.01.2022)

Deutsches Bundesministerium der Justiz und für Verbraucherschutz, Website <www.gesetze-im-internet.de/netzdg/index.html> (abgefragt am 14.01.2022)

Die Presse, Website 30.01.2020, Facebook wächst auf 2,5 Milliarden Nutzer <www.diepresse.com/5760750/facebook-wachst-auf-25-milliarden-nutzer> (abgefragt am 14.01.2022)

Die Presse, Website 01.07.2014, Vorratsdatenspeicherung in Österreich außer Kraft <www.diepresse.com/3830407/vorratsdatenspeicherung-in-osterreich-ausser-kraft> (abgefragt am 14.01.2022)

Europäische Union, Website, Gesetz über digitale Dienste: mehr Sicherheit und Verantwortung im Online-Umfeld <ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_de> (abgefragt am 14.01.2022)

Futurezone, Website 23.08.2012, Klarnamenzwang in Südkorea ist verfassungswidrig <www.futurezone.at/netzpolitik/klarnamenzwang-in-suedkorea-ist-verfassungswidrig/24.584.187> (abgefragt am 14.01.2022)

Kurier, Website 23.09.2020, Hass im Netz: ZARA verzeichnete starken Anstieg bei Meldungen <www.kurier.at/politik/inland/hass-im-netz-zara-verzeichnete-starken-anstieg-bei-meldungen/401041340> (abgefragt am 14.01.2022)

Neuwal.com, Website 13.11.2018, Transkript: Gernot Blümel bei Armin Wolf in der ZIB2 <www.neuwal.com/transkript/20181113-armin-wolf-gernot-bluemel-zib2.php> (abgefragt am 14.01.2022)

ORF.at, Website 13.11.2018, Regierung will „Vermummungsverbot“ <www.orf.at/stories/3100546> (abgefragt am 14.01.2022)

Süddeutsche Zeitung, Website 17.05.2019, Union für Klarnamenpflicht im Internet <www.sueddeutsche.de/politik/facebook-weber-schaeuble-klarnamen-1.4451908> (abgefragt am 14.01.2022)

8. Rechtsquellenverzeichnis

Österreichische Rechtsquellen

Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden

(E-Commerce-Gesetz – ECG), BGBl I 152/2001 idF I 148/2020

Bundesgesetz, mit dem Bestimmungen für privaten Hörfunk erlassen werden

(Privatradiogesetz – PrR-G), BGBl I 20/2001 idF I 86/2015

Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird

(Telekommunikationsgesetz 2003 – TKG 2003), BGBl I 70/2003 idF I 148/2021

Bundesgesetz, mit dem Maßnahmen zur Bekämpfung von Hass im Netz getroffen werden

(Hass-im-Netz-Bekämpfungs-Gesetz – HiNBG), BGBl I 148/2020

Bundesgesetz über die Förderung der Presse

(Presseförderungsgesetz 2004 – PresseFG 2004), BGBl I 136/2003 idF I 32/2018

Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen

(Kommunikationsplattformen-Gesetz – KoPl-G), BGBl I 151/2020

Bundesgesetz vom 12. Juni 1981 über die Presse und andere publizistische Medien

(Mediengesetz – MedienG), BGBl 314/1981 idF I 32/2018

Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener

Daten (Datenschutzgesetz – DSG), BGBl I 165/1999 idF I 14/2019

Kundmachung des Bundeskanzlers über die Aufhebung von Bestimmungen des Telekommunikationsgesetzes 2003, der Strafprozeßordnung 1975 und des

Sicherheitspolizeigesetzes durch den Verfassungsgerichtshof, BGBl I 44/2014

(kundgemacht am 30.06.2014)

Kundmachung der Bundeskanzlerin über die Aufhebung des § 54 Abs. 4b und des § 57 Abs. 2a des Sicherheitspolizeigesetzes, des § 98a Abs. 2 erster Satz der Straßenverkehrsordnung 1960 und des § 134 Z 3a und des § 135a der Strafprozeßordnung 1975 durch den Verfassungsgerichtshof, BGBl I 113/2019 (kundgemacht am 27.12.2019)

ME Bundesgesetz über Sorgfalt und Verantwortung im Netz (SVN-G), Erläuterungen, 134/ME XXVI. GP

<www.parlament.gv.at/PAKT/VHG/XXVI/ME/ME_00134/fname_747397.pdf>

(abgefragt am 14.01.2022)

ME Bundesgesetz über Sorgfalt und Verantwortung im Netz (SVN-G), Gesetzestext, 134/ME XXVI. GP

<www.parlament.gv.at/PAKT/VHG/XXVI/ME/ME_00134/fname_747395.pdf>

(abgefragt am 14.01.2022)

Verordnung der Bundesministerin für Justiz über den Ersatz der Kosten der Anbieter für die Mitwirkung an der Auskunft über Daten einer Nachrichtenübermittlung, der Auskunft über Vorratsdaten und der Überwachung von Nachrichten (Überwachungskostenverordnung – ÜKVO), BGBl II 322/2004

Europäische Rechtsquellen

Charta der Grundrechte der Europäischen Union, ABl C 2007/303, 1;
ABl C 2010/83, 389; ABl C 2012/326, 391; ABl C 2016/202, 389; BGBl III 132/2009

Erläuterungen zur Charta der Grundrechte (2007/C 303/02), ABl C 2007/303, 17

Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“), ABl L 2000/178, 1

Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation

(Datenschutzrichtlinie für elektronische Kommunikation), ABl L 2002/201, 37 idF ABl L 2009/337, 11

Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl L 2006/105, 54

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 2016/119, 1 idF ABl L 2021/074, 35

Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz -NetzDG) vom 1. September 2017, dBGBI I S 3352 idF I S 1436

9. Judikaturverzeichnis

Österreichische Judikatur

VfGH 11.12.2019, G 72-74/2019, G 181-182/2019

VfGH 27.06.2014, G 47/2012, G 59/2012, G 62/2012, G 70/2012, G 71/2012

VfGH 29.06.2012, B 1031/11 VfSlg 19.657/2012

OGH 15.09.2020, 6 Ob 195/19y

OGH 30.03.2020, 4 Ob 36/20b

OGH 22.06.2012, 6 Ob 119/11k

RIS-Justiz RS0127160: Unter Namen und Adresse eines Nutzers
iSd § 18 Abs 4 ECG sind grundsätzlich dessen Vor- und
Zuname und dessen Postanschrift aber auch dessen E-Mail-
Adresse zu verstehen.

RIS-Justiz RS0008985: Auch juristischen Personen kommt das Recht auf Ehre zu.

DSB 13.8.2018, D123.077/0003-DSB/2018

Europäische Judikatur

EGMR 04.12.2015, 47143/06 (GK) (*Roman Zakharov gg Russland*)

EGMR 16.06.2015, 64569/09 (GK) (*Delfi AS gg Estland*)

EGMR 04.12.2008, 30562/04 und 30566/04 (GK)

(S. und Marper gg Vereinigtes Königreich)

GA 18.11.2021, C-793/19, C-794/19 (*SpaceNet und Telekom Deutschland*)

GA 18.11.2021, C-14/20 (*Commissioner of the Garda Síochána u.a.*)

GA 18.11.2021, C-339/20, C-397/20 (*VD und SR*)

EuGH 02.03.2021, C-746/18 (*Prokuratuur*)

EuGH 06.10.2020, C-623/17 (*Privacy International*)

EuGH 03.10.2019, C-18/18 (*Glawischnig-Piesczek*)

EuGH 14.02.2019, C-345/17 (*Buivids*)

EuGH 21.12.2016, C-203/15, C-698/15 (*Tele2 Sverige und Watson u.a.*)

EuGH 08.04.2014, C-293/11, C-594/12 (*Digital Rights Ireland und Seitlinger u.a.*)

GA 12.12.2013, C-293/11, C-594/12 (*Digital Rights Ireland und Seitlinger u.a.*)

EuGH 16.12.2008, C-73/07 (*Satakunnan Markkinapörssi und Satamedia*)

10. Anhang

10.1 Anhang 1: Ministerialentwurf des SVN-G

Entwurf

Bundesgesetz, mit dem ein Bundesgesetz über Sorgfalt und Verantwortung im Netz erlassen und das KommAustria-Gesetz geändert wird

Der Nationalrat hat beschlossen:

Artikel 1

Bundesgesetz über Sorgfalt und Verantwortung im Netz (SVN-G)

1. Abschnitt

Allgemeine Bestimmungen

Gegenstand und Ziel dieses Gesetzes

§ 1. Mit diesem Bundesgesetz werden Maßnahmen festgelegt, mit denen alle diesem Gesetz unterliegenden Diensteanbieter von Postern in ihrem Forum verlangen, vorab ein Registrierungsprofil zu erstellen. Damit soll der respektvolle Umgang der Nutzer miteinander gefördert und die Verfolgung von Rechtsansprüchen erleichtert werden.

Begriffsbestimmungen

§ 2. Im Sinne dieses Bundesgesetzes bedeutet:

1. Dienst der Informationsgesellschaft: ein in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellter Dienst (§ 1 Abs. 1 Z 2 Notifikationsgesetz 1999, BGBl. I Nr. 183/1999), insbesondere der Online-Vertrieb von Waren und Dienstleistungen, Online-Informationsangebote, die Online-Werbung, elektronische Suchmaschinen und Datenabfragemöglichkeiten sowie Dienste, die Informationen über ein elektronisches Netz übermitteln, die den Zugang zu einem solchen vermitteln oder die Informationen eines Nutzers speichern (§ 3 Z 1 E-Commerce-Gesetz (ECG), BGBl. I Nr. 52/2001);
2. Diensteanbieter: ein Anbieter eines Dienstes der Informationsgesellschaft;
3. Forum: die online-Funktion zum Austausch von Mitteilungen oder Darbietungen mit gedanklichem Inhalt (Posting) von Nutzern mit einem größeren Personenkreis anderer Nutzer;
4. Poster: Nutzer, der in einem Forum ein Posting veröffentlicht.

2. Abschnitt

Anforderungen für Online-Informationsangebote

Registrierung und Authentifizierung

§ 3. (1) Diensteanbieter eines Online-Informationsangebotes haben, wenn sie

1. als Bestandteil des Dienstes selbst ein Forum einrichten und betreiben, das auf Nutzer in Österreich ausgerichtet ist, oder
2. im Rahmen ihres Dienstes die Einrichtung eines wie in Z 1 beschriebenen Forums durch die Nutzer ihres Dienstes ermöglichen,

von jedem Poster vorab zu verlangen, zur Authentisierung ein Registrierungsprofil zu erstellen.

- (2) Die Verpflichtungen nach Abs. 1 und nach den weiteren Bestimmungen dieses Abschnitts gelten
1. für Diensteanbieter, deren Dienst im Inland mehr als 100.000 registrierte Nutzer hat, sowie
 2. für Diensteanbieter, deren im vorangegangenen Jahr in Österreich erzielter Umsatz 500.000 Euro übersteigt;
 3. ferner für Medieninhaber, die im vorangegangenen oder aktuellen Kalenderjahr Fördermittel nach dem Presseförderungsgesetz, BGBl. I Nr. 136/2003 von mehr als 50.000 Euro erhalten haben oder erhalten und
 4. für mit einem nach Z 3 erfassten Medieninhaber im Sinne von § 9 Abs. 4 PrR-G, BGBl. I Nr. 20/2001 verbundene Diensteanbieter, soweit sie mit ihrem Online-Informationsangebot unter der gleichen oder einer ähnlichen Marke auftreten wie der nach Z 3 erfasste Fördermittelempfänger.

Zur Beurteilung, ob ein Diensteanbieter dem Anwendungsbereich unterliegt, hat er der RTR-GmbH bis spätestens 15. Jänner eines Jahres die Anzahl der registrierten Nutzer glaubhaft zu machen und die Umsätze des vorangegangenen Jahres zu melden. Im Fall des Verstreichens der Frist ist dem Diensteanbieter unter angemessener Fristsetzung eine Aufforderung zur Stellungnahme zu übermitteln, die auch eine Schätzung beinhaltet, ob die Nutzerzahlen und der Umsatz unter oder über dem Schwellenwert liegen. Erstattet der Diensteanbieter innerhalb der Frist weiterhin keine Meldung, liegt aber die angenommene Nutzerzahl und der geschätzte Umsatz über dem Schwellenwert, so ist davon auszugehen, dass das betreffende Unternehmen nicht ausgenommen ist. Ändern sich die Voraussetzungen, indem die Nutzerzahl oder der Umsatz unter dem Schwellenwert liegen, so hat der Diensteanbieter dies der RTR-GmbH mitzuteilen.

(3) Ausgenommen sind unabhängig von Nutzerzahl und Umsatz solche Online-Informationsangebote, bei denen nur für den Online-Verkauf oder -Tausch oder für die Online-Vermittlung von Waren oder Dienstleistungen, insbesondere mit Bewertungs-Möglichkeit oder Support-Funktion ein Forum eingerichtet oder betrieben wird.

(4) Im der Authentisierung dienenden Registrierungsprofil hat sich jeder Nutzer unter Angabe von Vorname, Nachname und Adresse als Poster zu registrieren. Dabei hat er einen Nutzernamen festzulegen, der im Forum als Bezeichnung für den Verfasser des Postings aufscheint. Dieser Nutzername muss nicht mit dem bürgerlichen Namen des Nutzers übereinstimmen. Der Diensteanbieter hat im Wege der Ausgestaltung des Vorgang der Registrierung für die Überprüfung der Identität des Nutzers auf der Grundlage von Dokumenten, Daten oder Informationen, die von einer glaubwürdigen und unabhängigen Quelle stammen, zu sorgen. Nach durchgeführter Überprüfung sind die für die Überprüfung verwendeten Dokumente und Informationen unverzüglich zu löschen.

Erst nach erfolgreichem Abschluss des Registrierungsprofils, darf der Diensteanbieter dem Nutzer die technische Möglichkeit gewähren, Beiträge in seinem Forum (§ 3 Abs. 1) zu erstellen. Vorname, Nachname und Adresse dürfen nur zum Zweck der Strafverfolgung durch kriminalpolizeiliche Behörden, Staatsanwaltschaften und Gerichte und zum Zweck der Rechtsverfolgung durch Dritte im Fall einer Privatanklage nach den §§ 111 und 115 StGB oder einer Klage nach § 1330 ABGB verarbeitet werden.

(5) Der Diensteanbieter hat Poster bei begründetem Verdacht auf unrichtige oder unrichtig gewordene Registrierungsangaben zum Nachweis der Richtigkeit der Angaben binnen angemessener Frist bei sonstiger Löschung des Registrierungsprofils aufzufordern und Nutzer mit offenkundig unrichtigen Angaben von vornherein von der Registrierung auszuschließen.

- (6) Der Diensteanbieter hat das Registrierungsprofil zu löschen
1. auf Verlangen des Posters,
 2. bei Abmeldung des Posters vom Online-Informationsangebot und
 3. jedenfalls bei im Rahmen von routinemäßig periodisch vorgenommenen Überprüfungsvorgängen festgestellter Inaktivität von mehr als einem Jahr.

Übermittlungspflichten

§ 4. (1) Der Diensteanbieter hat Vorname, Nachname sowie die Adresse des Posters einer dritten Person auf deren begründetes schriftliches Verlangen bekannt zu geben.

(2) Ein begründetes Verlangen im Sinne des Abs. 1 liegt nur dann vor, wenn die dritte Person unter Nachweis ihrer Identität glaubhaft macht, dass die Feststellung der Identität des Posters eine unabdingbare Voraussetzung bildet, um wegen des Inhalts eines Postings gegen diesen Poster mittels Privatanklage wegen übler Nachrede (§ 111 Abs. 2 StGB) oder wegen Beleidigung (§ 115 StGB) strafgerichtlich oder wegen Verletzungen an der Ehre (§ 1330 ABGB) zivilgerichtlich vorzugehen.

(3) Der Diensteanbieter hat ferner Vorname, Nachname sowie die Adresse des Posters auf Ersuchen von kriminalpolizeilichen Behörden, Staatsanwaltschaften und Gerichten, die sich auf die Aufklärung deskonkreten Verdachts einer durch den Inhalt eines Postings begangenen Straftat des Posters beziehen, bekannt zu geben.

(4) Bei begründeten Hinweisen, dass durch den Inhalt eines Postings der objektive Tatbestand der üblen Nachrede oder der Beleidigung hergestellt worden sein könnte oder dass der Inhalt sonst den konkreten Verdacht einer Straftat begründen könnte, hat der Diensteanbieter von dem betreffendenPosting eine Aufzeichnung herzustellen, die eine vollständige und originalgetreue Wiedergabe ermöglicht. Über ein Verlangen nach Abs. 2 oder ein Ersuchen nach Abs. 3 hat er auch diese näher bezeichnete Aufzeichnung zur Verfügung zu stellen. Beim Diensteanbieter darf keine Verknüpfung zwischen der Identität eines Posters und dem Inhalt eines Postings vorgenommen werden.

Verantwortlicher Beauftragter

§ 5. (1) Zur Sicherstellung ihrer Erreichbarkeit und als Zustellungsbevollmächtigten haben Diensteanbieter einen verantwortlichen Beauftragten zu bestellen, dem für die auf das Inland bezogene Tätigkeit des Unternehmens die Verantwortung für die Einhaltung der den Diensteanbietern auferlegten Pflichten obliegt. Die Aufsichtsbehörde ist unverzüglich über die Bestellung zu informieren.

(2) Die Kontaktdaten (Adresse, Telefonnummer, Email-Adresse) des verantwortlichen Beauftragten sind vom Diensteanbieter ständig leicht und unmittelbar auffindbar zur Verfügung zu stellen. Der Diensteanbieter hat die unverzügliche Erreichbarkeit des verantwortlichen Beauftragten sicherzustellen.

(3) Der verantwortliche Beauftragte hat sich für eine Zustellung mit Zustellnachweis durch einen Zustelldienst iSd §§ 33 und 35 des Zustellgesetzes, BGBl. Nr. 200/1982, anzumelden, und bei der Anmeldung mitzuteilen, dass es keine Zeiträume gibt, innerhalb derer die Zustellung ausgeschlossen sein soll.

(4) Zu verantwortlichen Beauftragten können nur natürliche Personen bestellt werden, die alle Voraussetzungen gemäß § 9 Abs. 4 des Verwaltungsstrafgesetzes 1991 (VStG), BGBl. Nr. 52/1991, erfüllen und insbesondere über eine für die Einhaltung der Bestimmungen dieses Bundesgesetzes erforderliche Anordnungsbefugnis verfügen.

3. Abschnitt

Aufsicht und Durchsetzung

Aufsichtsbehörde

§ 6. (1) Mit den in diesem Bundesgesetz der Aufsichtsbehörde übertragenen Aufgaben ist die gemäß § 1 des KommAustria-Gesetzes, BGBl. I Nr. 32/2001, eingerichtete Kommunikationsbehörde Austria betraut.

(2) Die Aufsichtsbehörde hat die Einhaltung und Umsetzung der in § 3 Abs. 4 und 5 vorgesehenen Verpflichtungen durch die Diensteanbieter stichprobenartig zu überprüfen. Die Diensteanbieter haben der Aufsichtsbehörde auf deren Verlangen alle hierzu erforderlichen Auskünfte zu erteilen.

(3) Die administrative Unterstützung der KommAustria in Angelegenheiten dieses Bundesgesetzes obliegt der RTR-GmbH unter der Verantwortung des Geschäftsführers für den Fachbereich Medien.

Geldbußen

§ 7. (1) Die Aufsichtsbehörde hat je nach Schwere des Vergehens eine Geldbuße bis zu 500.00 Euro, im Wiederholungsfall bis zu 1.000.000 Euro über einen Diensteanbieter zu verhängen, wenn dieser

1. eine der in § 3 Abs. 1 letzter Satz und Abs. 4 normierten Vorgaben bei der erstmaligen Registrierung nicht erfüllt;
2. entgegen § 3 Abs. 4 im Falle eines begründeten Verlangens gemäß § 4 Abs. 2 oder eines Ersuchens nach § 4 Abs. 3 nicht in der Lage ist, Auskunft über die Identität eines Posters zu erteilen;
3. einer der in § 3 Abs. 5 geregelten Verpflichtungen nicht entspricht;
4. der in § 3 Abs. 6 geregelten Verpflichtung nicht entspricht;
5. einer der in § 4 geregelten Pflichten zur Übermittlung von Daten nicht entspricht;
6. der in § 5 Abs. 1 geregelten Verpflichtung zur Bestellung eines Beauftragten oder der Verpflichtung zur unverzüglichen Information über die Bestellung nicht entspricht;

7. der in § 5 Abs. 2 geregelten Verpflichtung zur Bereitstellung der Kontaktdaten des Beauftragten nicht entspricht oder nicht sicherstellt, dass der Beauftragte unverzüglich erreichbar ist;
 8. der Pflicht zur Auskunftserteilung gemäß § 6 Abs. 2 nicht entspricht.
- (2) Bei der Bemessung der Höhe einer Geldbuße sind insbesondere folgende Umstände zu würdigen:
1. Finanzkraft des Diensteanbieters, wie sie sich beispielsweise aus dem Gesamtumsatz der verantwortlichen juristischen Person oder den Jahreseinkünften der verantwortlichen natürlichen Person ablesen lässt;
 2. frühere Verstöße;
 3. das Ausmaß und die Dauer der Nachlässigkeit des Diensteanbieters bei der Einhaltung der aufgetragenen Verpflichtung;
 4. der Grad der Intentionalität des Verstoßes;
 5. der Beitrag zur Wahrheitsfindung sowie
 6. das Ausmaß der getroffenen Vorkehrungen zur Verhinderung eines Verstoßes oder der Anleitung der Mitarbeiter zu rechtstreuem Verhalten.

Geldstrafen

§ 8. (1) Wer als verantwortlicher Beauftragter der in § 5 Abs. 3 geregelten Verpflichtung nicht entspricht, begeht eine Verwaltungsübertretung und ist mit einer Geldstrafe bis zu 10.000 Euro zu bestrafen.

(2) Wer als verantwortlicher Beauftragter nicht dafür sorgt, dass ein Diensteanbieter den Verpflichtungen nach § 3 Abs. 1 und 4 oder § 3 Abs. 5 entspricht, begeht eine Verwaltungsübertretung und ist mit einer Geldstrafe bis zu 100.000 Euro zu bestrafen.

(3) Die Aufsichtsbehörde hat von der Bestrafung des verantwortlichen Beauftragten abzusehen, wenn für denselben Verstoß bereits eine Geldbuße über die juristische Person verhängt wurde und keine besonderen Umstände vorliegen, die einem Absehen von der Bestrafung entgegenstehen.

Ausnahme von der Verantwortlichkeit

§ 9. Über den Diensteanbieter ist keine Geldbuße zu verhängen und der verantwortliche Beauftragte ist nicht zu bestrafen, wenn eine Identifikation des Posters als Voraussetzung eines gegen diesen Poster gerichteten gerichtlichen Verfahrens zwar scheitert, der Diensteanbieter aber glaubhaft machen kann, dass er mit allen ihm zur Verfügung stehenden Mitteln für eine Überprüfung der Identität gesorgt hat.

4. Abschnitt

Schlussbestimmungen

Verweisungen und Bezeichnungen

§ 10. (1) Soweit in diesem Bundesgesetz auf andere Bundesgesetze verwiesen wird, sind diese in ihrer jeweils geltenden Fassung anzuwenden.

(2) Alle in diesem Bundesgesetz verwendeten personenbezogenen Bezeichnungen gelten gleichermaßen für Personen weiblichen als auch männlichen Geschlechts.

(3) Die nach diesem Bundesgesetz verhängten Geldbußen und Geldstrafen fließen dem Bund zu und sind nach den Bestimmungen über die Eintreibung von gerichtlichen Geldstrafen einzubringen. Rechtskräftige Bescheide sind Exekutionstitel. Von den Geldbußen sind jeweils jährlich 50vH für Zwecke der Erfüllung der in diesem Bundesgesetz vorgesehenen Aufgaben der Aufsichtsbehörde und der administrativen Unterstützung durch die RTR-GmbH zu verwenden und zuzuweisen.

Vollziehung

§ 11. Mit der Vollziehung dieses Bundesgesetzes ist der Bundeskanzler betraut.

Inkrafttreten und Übergangsbestimmungen

§ 12. Dieses Bundesgesetz tritt mit 1. September 2020 in Kraft. Die zum Zeitpunkt des Inkrafttretens dieses Bundesgesetzes tätigen Diensteanbieter müssen, soweit sie nicht gemäß § 3 Abs. 3 vom Anwendungsbereich ausgenommen sind, die in § 5 Abs. 1 vorgesehene Bestellung bis zum 31. März 2020, später hinzutretende Diensteanbieter, soweit sie nicht gemäß § 3 Abs. 3 vom Anwendungsbereich ausgenommen sind, innerhalb von drei Monaten ab der Aufnahme der Tätigkeit umgesetzt haben. Abweichend von § 3 Abs. 2 haben Diensteanbieter, die von § 3 Abs. 1 erfasst sind, der RTR-GmbH erstmals bis 31. Oktober 2020 glaubhaft zu machen, dass sie im vorangegangenen Kalenderjahr eine Nutzerzahl oder einen Umsatz unter dem jeweiligen Schwellenwert aufgewiesen haben.

Artikel 2

Änderung des KommAustria-Gesetzes

Das KommAustria-Gesetz, BGBl. I Nr. 32/2001, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 78/2018, wird wie folgt geändert:

1. In § 2 Abs. 1 wird am Ende der Z 12 der Punkt durch einen Beistrich ersetzt und folgende Z 13 angefügt:

„13. Wahrnehmung der Aufgaben nach dem Bundesgesetz über Sorgfalt und Verantwortung im Netz (SVN-G), BGBl. I Nr. xxx/2019.“

2. In § 13 Abs. 4 wird am Ende der Z 3 der Punkt durch einen Strichpunkt ersetzt und folgende Z 4 angefügt:

„4. Wahrnehmung der Aufgaben nach dem SVN-G.“

3. In § 17 Abs. 1 wird am Ende der Z 4 der Punkt durch einen Strichpunkt ersetzt und folgende Z 5 angefügt:

„5. die fachliche und administrative Unterstützung in Angelegenheiten nach dem SVN-G.“

4. Nach § 35 wird folgender § 35a samt Überschrift eingefügt:

„Finanzierung des Aufwands der Aufsicht über Online-Informationsangebote

§ 35a. Der in Erfüllung der Aufgabe nach § 2 Abs. 1 Z 13 entstehende Aufwand der KommAustria sowie der RTR-GmbH im Fachbereich Medien zur Unterstützung der KommAustria ist aus dem sich nach § 35 Abs. 1 Satz 2 errechnenden Zuschuss aus dem Bundeshaushalt zu bestreiten.“

5. Dem § 44 wird folgender Abs. 22 angefügt:

„(22) § 2 Abs. 1, § 13 Abs. 4, § 17 Abs. 1 und § 35a in der Fassung des Bundesgesetzes BGBl. I Nr. xxx/2019 treten mit 1. September 2020 in Kraft.“

10.2 Anhang 2: Erläuterungen zum Ministerialentwurf des SVN-G

Erläuterungen Allgemeiner Teil

Hauptgesichtspunkte des Entwurfs

In der digitalen Welt müssen die gleichen Prinzipien gelten, wie in der real gelebten Welt. Das Internet kann und darf kein rechtsfreier Raum sein und den leider vermehrt vorkommenden klaren Grenzüberschreitungen, Herabwürdigungen, Demütigungen und Übergriffen sollen mit diesem Gesetz wirksame rechtliche Maßnahmen gegenübergestellt werden. Grundprinzipien, Regeln und Gesetze müssen auch im digitalen Raum gelten. Was in der analogen Welt geahndet wird, muss auch in der digitalen Welt Folgen haben.

Sich in der Anonymität des Internets verstecken zu können, darf in Fällen, in denen Straftaten begangen werden, nicht mehr möglich sein. Denn nur wenn durch eine Authentifizierung auch die Identifizierung der Täter bei Rechtsverletzungen möglich ist, werden die gleichen Maßstäbe wie auch in der analogen Welt gelten können. Eine wirksame Authentifizierung zur Bestätigung der Nutzerdaten ist dabei unumgänglich.

Der vorliegende Entwurf geht davon aus, dass der Diensteanbieter sicherstellen muss, dass Personen im Anlassfall identifizierbar sind. Daran anknüpfend überlässt es der Entwurf aber dem Diensteanbieter sich eines Systems zu bedienen, das in einem stufenweisen Ansatz – neben der Möglichkeit der Verfolgung von Officialdelikten – auch dann eine Identifikation ermöglicht, wenn es um die Fälle der §§ 111 und 115 StGB und des § 1330 ABGB geht und dritte Personen die Identität eines Posters für die Verfolgung ihrer Privatanlage oder ihrer zivilrechtlichen Ansprüche herausfinden müssen.

Zur Förderung des respektvollen Umgangs der Poster in online-Foren miteinander und zur Erleichterung der Verfolgung von Rechtsansprüchen im Falle tatsächlich rechtswidriger Postings sind daher insbesondere folgende Maßnahmen vorgesehen:

- ☐ Verpflichtung der Diensteanbieter, die Foren betreiben bzw. die Einrichtung eines Forums ermöglichen, dafür Sorge zu tragen, dass die Identität des Posters festgestellt und überprüft wird. Erst nach erfolgreichem Abschluss des Registrierungsprofils kann der Nutzer Postings in diesem Forum veröffentlichen.
- ☐ Nutzer haben ein Registrierungsprofil zu erstellen und sich zu identifizieren.
- ☐ Verpflichtung der Diensteanbieter zur Bestellung eines verantwortlichen Beauftragten, insbesondere als Zustellbevollmächtigtem.
- ☐ Sicherstellung einer der DSGVO entsprechenden Datenverarbeitung und Übermittlungsverpflichtung an Gerichte, Staatsanwaltschaft, insbesondere aber auch an Dritte in spezifisch im Gesetz aufgezählten Fällen.
- ☐ KommAustria als Aufsichtsbehörde kann Geldbußen gegen Diensteanbieter und Geldstrafen über von diesen zu bestellende verantwortliche Beauftragte verhängen.

Der im Entwurf gewählte Ansatz beruht auf der Tatsache, dass es bereits verschiedene Beispiele von verschiedenen Anbietern von Foren gibt, bei denen sich der User „verifizieren“ lassen kann, etwa indem er einen geeigneten Identitätsnachweis vorlegt.

Der Entwurf wird im Vorhinein der Kommission zu notifizieren sein, weil er nicht der Umsetzung von Unionsrecht dient, aber in einen Kernbereich des Unionsrechts fällt: Gemäß der Richtlinie (EU) 2015/1535 müssen die Mitgliedstaaten die Kommission über jeden Entwurf einer technischen Vorschrift zu einem Dienst der Informationsgesellschaft **vor deren Erlass** unterrichten und grundsätzlich eine dreimonatige Stillhaltefrist abwarten, um der Kommission und den anderen Mitgliedstaaten zu ermöglichen, den notifizierten Wortlaut zu prüfen und angemessen zu reagieren. Die E-Commerce Richtlinie lässt unter bestimmten Voraussetzungen den Mitgliedstaaten die Möglichkeit, Maßnahmen auch gegenüber ausländischen Anbietern zu ergreifen, wenn dies zum Schutz der öffentlichen Ordnung, insbesondere Verhütung, Ermittlung, Aufklärung und Verfolgung von Straftaten, einschließlich des Jugendschutzes und der Bekämpfung der Hetze aus Gründen der Rasse, des Geschlechts, des Glaubens oder der Nationalität, sowie von Verletzungen der Menschenwürde einzelner Personen notwendig ist und die Maßnahmen in einem angemessenen Verhältnis zu diesen Schutzziele stehen.

In Bezug auf die verfahrensrechtlichen Konsequenzen ist auf die Spruchpraxis des Gerichtshofs der Europäischen Union hinzuweisen: Nach dem Urteil in der Rechtssache „CIA Security“ vom 30. April 1996, kann eine nationale Vorschrift, die nicht nach dem 98/34-Richtlinienverfahren (nunmehr

2015/1535) notifiziert wurde, obwohl dies Pflicht gewesen wäre, von nationalen Gerichten für unanwendbar erklärt werden. Ähnliches gilt nach dem Urteil in der Rechtssache „Unilever“ vom 26. September 2000, gemäß dem eine technische Vorschrift, die unter Verstoß gegen die Verpflichtung zur Verschiebung der Annahme einer notifizierten nationalen Rechtsvorschrift, d. h. zur Einhaltung der Stillhaltefrist, erlassen wurde, ebenfalls von nationalen Gerichten für unanwendbar auf Einzelne erklärt werden kann (vgl. dazu <http://ec.europa.eu/growth/tools-databases/tris/de/about-the-20151535/the-notification-procedure-in-brief1/> zuletzt abgerufen am 10. April 2019).

Kompetenzgrundlage

Die Zuständigkeit des Bundes zur Erlassung dieses Bundesgesetzes ergibt sich aus Art. 10 Abs. 1 Z 6B-VG („Pressewesen“) und Z 9 B-VG („Post- und Fernmeldewesen“).

Besonderer Teil

Zu § 1:

Dem Wesen einer Zielbestimmung entsprechend kommt den gewählten Formulierungen kein normativer Gehalt zu. Die Ausführungen dienen vielmehr der Kurzdarstellung des Inhalts und sind als neben die üblichen Auslegungsmethoden tretendes Instrument für die Interpretation der normativ formulierten Vorgaben für die Festlegung von Maßnahmen zu verstehen.

Zu § 2:

Die Definitionen in Z 1 und 2 geht auf wortidentische unionsrechtlich vorgegebene Begrifflichkeiten zurück und übernehmen den Wortlaut des den Art. 2 der E-Commerce-Richtlinie umsetzenden § 3 des österreichischen E-Commerce-Gesetzes. Die Regelungen des Entwurfs sollen auf in- und ausländische Anbieter zur Anwendung kommen, soweit diese, was sich aus der Anordnung in § 3 Abs. 1 ergibt, ein auch auf das Publikum in Österreich ausgerichtetes Forum betreiben.

Die Dienste der Informationsgesellschaft (Z 1) sind ein zentraler Begriff der E-Commerce-Richtlinie. Diese Richtlinie behandelt elektronische „Angebote“, die im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellt werden. Der vorliegende Entwurf umschreibt diese Dienste in Anlehnung an die im Wesentlichen gleichlautenden Legaldefinitionen des § 1 Abs. 1 Z 2 des Notifikationsgesetzes 1999 und des § 2 Z 5 des Zugangskontrollgesetzes als „in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf bereitgestellten Dienst“. Was diese Definitionselemente genau besagen, ergibt sich aus § 1 Abs. 1 Z 2 NotifG 1999, auf den ausdrücklich verwiesen wird. Auch § 3 ECG geht auf diese Definitionen zurück und zählt in der Folge einige besonders wichtige Online-Dienste auf, die Dienste der Informationsgesellschaft sind. Diese – demonstrative – Aufzählung soll das Gesetz anschaulicher und verständlicher machen (vgl. auch die in Erwägungsgrund 18 der E-Commerce-Richtlinie erwähnten Beispiele). Wenn etwa ein Unternehmer nur mittels der elektronischen Post kommuniziert, ohne dass er weitere elektronische Mittel verwendet, stellt dieser Einsatz der elektronischen Post noch keinen Dienst der Informationsgesellschaft dar. Wenn sich aber an die Verwendung der elektronischen Post weitere elektronische Vertriebsformen knüpfen (etwa eine Homepage des Unternehmers), so fällt das Angebot unter die Begriffsbestimmung. Gleiches gilt für die Bereitstellung eines Online-Foren, allerdings immer unter der Voraussetzung, dass sämtliche Definitionselemente erfüllt werden. Ein elektronischer Dienst, der dem Entwurf unterliegt, muss „in der Regel gegen Entgelt“ bereitgestellt werden. Bei den Diensten der Informationsgesellschaft handelt es sich – grob umrissen – um kommerzielle elektronische Dienste, um Dienste, die in Ertragsabsicht erbracht werden. Nach der Rechtsprechung des Europäischen Gerichtshofs muss das Entgelt die wirtschaftliche Gegenleistung für die bereitgestellte Leistung darstellen (vgl. EuGH 7. 12. 1993, Rs C-109/92, *Wirth*, Slg. 1993, I-6447). An dieser Voraussetzung fehlt es bei Tätigkeiten, die die öffentliche Hand ohne wirtschaftliche Gegenleistung im Rahmen ihrer Aufgaben, vor allem in den Bereichen Soziales, Kultur, Bildung und Justiz, ausübt. Solche Dienstleistungen zählen nicht zu den Diensten der Informationsgesellschaft. Dies gilt auch dann, wenn diese Aktivitäten von Selbstverwaltungskörpern (etwa einer Kammer oder einem Sozialversicherungsträger) ausgeübt werden.

Auch sind – private oder staatliche – Dienste, die keinen ökonomischen Hintergrund aufweisen (wie etwa von Universitäten betriebene und der Öffentlichkeit zur Verfügung stehende Datenbanken), keine Dienste der Informationsgesellschaft. Ebenso sind die Verwendung der elektronischen Post zwischen Privatpersonen außerhalb ihrer geschäftlichen, gewerblichen oder beruflichen Tätigkeit und die reine Verwendung der elektronischen Post im geschäftlichen Verkehr keine Dienste der Informationsgesellschaft.

Der Ausdruck „in der Regel gegen Entgelt“ entspricht der Terminologie des Unionsrechts (vgl. dazu und für die folgenden Überlegungen auch die Erl zur RV zum E-Commerce-Gesetz). Auslegungsprobleme können sich im Zusammenhang mit dem Entgeltlichkeitserfordernis dann ergeben, wenn – wie es gerade im Internet häufig der Fall ist – zunächst unentgeltlich Leistungen zur Verfügung gestellt werden und der

Nutzer erst dann ein Entgelt entrichten muss, wenn er eine vorerst unentgeltlich in Anspruch genommene Leistung weiter beziehen will. Im Allgemeinen wird hier eine Gesamtschau anzustellen sein, sodass auch die unentgeltlich angebotenen Leistungen schon Bestandteil eines Dienstes der Informationsgesellschaft sind. Ferner ist es nicht erforderlich, dass ein Nutzer für jede einzelne Dienstleistung ein Entgelt entrichtet. Vielmehr liegt auch dann ein Dienst der Informationsgesellschaft vor, wenn eine einzelne Leistung unentgeltlich abgerufen werden kann, diesem Abruf aber eine – entgeltliche – Rahmenbeziehung zugrunde liegt. Darüber hinaus ist es nicht geboten, dass die Dienste von demjenigen vergütet werden, der sie empfängt (siehe auch den Erwägungsgrund 18 der E-Commerce-Richtlinie). Auch eine von einem Sponsor finanzierte, vom Nutzer unentgeltlich abrufbare Website, der Betrieb einer mit Werbung unterlegten elektronischen Suchmaschine oder die Werbung selbst kann daher ein Dienst der Informationsgesellschaft sein. Der Dienst der Informationsgesellschaft muss „im Fernabsatz“ erbracht werden. Der Diensteanbieter und der Empfänger (oder deren Vertreter) dürfen also nicht gleichzeitig körperlich anwesend sein.

Der Dienst der Informationsgesellschaft muss ferner „elektronisch“ erbracht werden. Die Daten oder Informationen müssen über ein System laufen, in dem die Daten sowohl beim Sender als auch beim Empfänger elektronisch verarbeitet und gespeichert werden. Dabei müssen die elektronischen Daten gesendet, weitergeleitet und empfangen werden. Charakteristisch ist, dass die Daten von „Punkt zu Punkt“ übertragen werden. Solche Dienste der Informationsgesellschaft sind etwa – wie auch schon in § 3 Z 1 ECG in teilweiser Anlehnung an den Erwägungsgrund 18 der E-Commerce-Richtlinie verdeutlicht werden sollte – das so genannte „electronic publishing“, die Online-Werbung und andere elektronische Maßnahmen zur Absatzförderung, Online-Informationsangebote sowie Online-Dienste, die Instrumente zur Datensuche, zum Zugang zu Daten oder zur Datenabfrage bereitstellen. Letztlich müssen die Dienste der Informationsgesellschaft individuell abrufbar sein. Der jeweilige Nutzer muss also in der Lage sein, den Inhalt des Dienstes (die Informationen oder Kommunikationsdaten) gesondert in Anspruch zu nehmen. Nicht individuell abrufbar sind Dienste, die gleichzeitig für eine unbegrenzte Zahl von Empfängern bereitgestellt werden, wie bei linearen Diensten (etwa Fernseh-, Radio- und Teletextdienste).

Zu § 3:

Abs. 1 legt den Kreis der zur Sicherstellung der Registrierung und Authentifizierung ihrer Nutzer – konkret nur jener Personen, die sich als Poster in einem Forum durch Teilnahme an „Debatten“ beteiligen wollen – verpflichteten Diensteanbieter fest. Es handelt sich dabei um in- und ausländische Anbieter von Online-Informationsangeboten (wie in ErwG 21 der E-Commerce-Richtlinie angeführt), die (ergänzend) zu ihrem Informationsangebot auch die Funktion eines Forums entweder selbst bereitstellen oder ihren Nutzern die Möglichkeit einräumen, gleichsam zur Kommentierung der online angebotenen Informationen ein Forum einzurichten. Selbstverständlich sollen die Regelungen nicht auf sämtliche Foren weltweit Anwendung finden, sondern der gegenständliche Entwurf verlangt ausdrücklich einen klaren Konnex zu Österreich, weil nur Poster und Foren erfasst werden, die zB durch den Inhalt, die Zielgruppe, die Sprache als auf Nutzer in Österreich ausgerichtet qualifiziert werden können. Das etwa von einem Zeitungsunternehmen in Frankreich bereitgestellte Forum zur Kommentierung des Webangebots der französischen Zeitung fällt daher selbstverständlich auch dann nicht unter den Anwendungsbereich, wenn sich „österreichische“ Nutzer in diesem Forum beteiligen oder auf Österreich bezogene Inhalte vorzufinden sind. Wird aber von einem ausländischen Online-Informationsanbieter ein Forum geschaffen (oder etwa durch Tools oder Apps dem Nutzer die Möglichkeit eröffnet, ein Forum einzurichten), das auf den österreichischen Markt abzielt, indem es einen Marktplatz für den Meinungsaustausch in Österreich einräumt, so soll der betreffende Diensteanbieter den Verpflichtungen des vorliegenden Entwurfs unterliegen. Für die Beurteilung der Frage, ob ein Dienst auf Österreich ausgerichtet ist, können etwa Werbeeinnahmen, die im Zusammenhang mit einem bestimmten Online-Angebot in Österreich generiert werden, als Anknüpfungspunkt herangezogen werden. Ein angebotenes Forum (dh. „sein“ Diensteanbieter) fällt aber nicht schon deswegen aus dem Anwendungsbereich heraus, weil in dem Forum europäische oder internationale Themen zur Debatte gestellt werden, die mit Österreich nichts oder wenig zu tun haben.

Abs. 2 liegt der Grundgedanke der Zumutbarkeit einer Verpflichtung zur Inanspruchnahme und Einrichtung technischer Maßnahmen zugrunde. Die Verpflichtung, von den Nutzern eine Registrierung zu verlangen, soll daher bei Diensteanbietern nur dann greifen, wenn sie eine relevante Größe – ausgedrückt durch eine Umsatzschwelle und eine Anzahl von registrierten Nutzern – erreicht haben. In den Anwendungsbereich einbezogen werden auch – weil sie besonders als zur Vielfalt der Meinungsbildung beiträgend angesehen werden – solche Medieninhaber, die – was sich aus dem Zusammenhalt mit Abs. 1 ergibt – Anbieter von Foren sind und höhere Zuwendungen aus dem Titel der Presseförderung erhalten. Schließlich werden solche Unternehmen, die Foren bereitstellen, erfasst, wenn sie in qualifizierter Weise

mit einem solchen Förderungsempfänger verbunden sind und unter der gleichen oder einer ähnlichen Marke wie jener des Förderungsempfängers auftreten.

Abs. 3 normiert unter der Annahme, dass die darin beschriebenen Dienste aufgrund ihrer von vorneherein bestehenden thematischen Eingrenzung keine Gelegenheit bieten, inhaltlich problematische dh. insbesondere den Persönlichkeitsschutz beeinträchtigende Darstellungen zu veranlassen, sachlich rechtfertigbare Ausnahmen.

Filehosting-Dienste (auch Cloud Storage genannt), bei denen man Dateien in einen speziellen Ordner ablegt und dieser Ordner im Hintergrund mit einem auf dem Server eingerichteten Ordner abgeglichen wird, sobald man sich mit einem weiteren Computer mit demselben Konto anmeldet, womit ebenso automatisch im Hintergrund der Server-Ordner mit dem entsprechenden Ordner auf dem anderen PC abgeglichen wird, fallen nicht in den Anwendungsbereich. Der Anwender legt nur seine Dateien in den lokalen Ordner und im Hintergrund wird automatisch abgeglichen. Unter die Ausnahme fallen auch Portale, die etwa Reisen oder Hotelzimmer vermitteln, selbst wenn sie ein Forum betreiben, dessen Inhalte aber im weitaus überwiegendem Ausmaß auf die Bewertung der Qualität der Reise oder des Aufenthalts beschränkt sein werden und keinen spezifischen Anlass für Verletzungen des Persönlichkeitsschutzes bieten. Andererseits fallen aber Internetauftritte wie etwa Arztbewertungsportale

– die selbst keine Dienstleistungen vermitteln, sondern Benutzern die Möglichkeit geben, Ärzte und andere Angehörige von Heilberufen zu bewerten – als Online-Informationsangebote mit einem Forum (Kommentarfunktion) in den Anwendungsbereich (so sie die Kriterien nach Abs. 2 erfüllen); auch sie ermöglichen subjektive Bewertungen und Äußerungen.

Abs. 4 verpflichtet die diesem Gesetz unterliegenden Diensteanbieter dazu, für die Feststellung und Überprüfung der Identität des Posters Sorge zu tragen. Wie dies bewerkstelligt wird, bleibt dem Diensteanbieter überlassen. Die Verpflichtung des Diensteanbieters wäre beispielsweise dann erfüllt, wenn die für die Rechtsverfolgung notwendigen Daten mittels 2-Faktor-Authentifizierung mit Mobiltelefonnummer bestätigt werden oder der Diensteanbieter sichergestellt hat, dass er – gegebenenfalls in Kooperation mit dem Betreiber des Telefondienstes – bei begründeten Anfragen, die für die Rechtsverfolgung notwendigen Daten in Erfahrung bringen kann.

Inhaltlich und sprachlich ist zwischen der Authentisierung und der Authentifizierung zu unterscheiden (vgl. dazu näher und die folgenden Zitate aus <https://www.datenschutzbeauftragter-info.de/authentisierung-authentifizierung-und-autorisierung/>, zuletzt abgerufen am 14. Februar 2019): Die Authentisierung stellt den Nachweis einer Person dar, dass sie tatsächlich diejenige Person ist, die sie vorgibt zu sein. Eine Person legt also Nachweise vor, die ihre Identität bestätigen sollen. Demgegenüber stellt die Authentifizierung „eine Prüfung der behaupteten Authentisierung dar. Zeitlich betrachtet findet eine „Authentifizierung“ also nach einer „Authentisierung“ statt.“

Durch Verpflichtung des Diensteanbieters soll in letzter Konsequenz ausgehend von der Registrierung in mehreren Schritten die Feststellung der Identität des des/der Poster/s/in – allerdings eingeschränkt auf spezifisch im vorliegenden Entwurf geregelte Fälle – ermöglicht werden.

Zur Bewertung der Eignung, Notwendigkeit und Verhältnismäßigkeit ist festzuhalten, dass die im SVN-G enthaltenen Regelungen über die Ermittlung und Speicherung von Daten und die damit verbundene Auswirkung auf die „Anonymität“ des Äußernden einem von Art. 10 Abs. 2 EMRK anerkannten Ziel, nämlich dem Schutz der Rechte Dritter durch die Verbesserung der Verfügbarkeit der Daten im Falle von Verletzungen von Bestimmungen zum Persönlichkeitsschutz dienen. Es bedarf angesichts der verschiedenen im Entwurf vorgesehenen Vorkehrungen auch keiner weiteren Ausführungen, dass von einer Aufhebung der Anonymität nicht die Rede sein kann, sondern die Regelungen des Entwurfs einen angemessenen Ausgleich zwischen dem Recht auf Meinungsäußerungsfreiheit einerseits und dem Recht auf Schutz des guten Rufs und Sicherstellung des Persönlichkeitsschutzes andererseits bewirken sollen. Die Notwendigkeit ergibt sich aus dem wichtigen öffentlichen Interesse an einer erfolgreichen Rechtsverfolgung in den spezifisch genannten Fällen auch durch Dritte, die ohne die Verfügbarkeit der betreffenden Daten scheitert. Gesondert ist darauf hinzuweisen, dass – wie § 4 Abs. 4 des Entwurfs dies eindeutig regelt – beim Diensteanbieter keinerlei Verknüpfung zwischen der Identität eines Posters und dem Inhalt eines Postings vorgenommen werden darf und die Daten überhaupt nur in konkret bezeichneten Fällen, dh. nur ausnahmsweise „herausgeben“ darf. Auch bei der Art der Daten geht der Entwurf davon aus, dass nicht mehr als Vor- und Nachname sowie Wohnadresse notwendig sind, um die Rechtsverfolgung sicherzustellen.

Der Diensteanbieter hat im Sinne des Abs. 5 den Nutzer bei begründetem Verdacht, dass die Registrierungsangaben unrichtig sind oder wurden (etwa weil das Registrierungsprofil nicht mehr eindeutig zuordenbar ist) zum Nachweis der Richtigkeit der Angaben aufzufordern. Ein begründeter Verdacht wird erst dann vorliegen, wenn aufgrund bestimmter objektiver Anhaltspunkte angenommen

werden kann, dass eine falsche Angabe vorliegt. Das bedeutet, es muss ein hinreichender Anlass (aufgrund bestimmter, jedenfalls nachprüfbarer oder widerlegbarer Anhaltspunkte) für die Annahme gegeben sein. Eine bloße Vermutung reicht daher nicht. Der Diensteanbieter hat dabei durch routinemäßig periodisch vorgenommene Überprüfungsvorgänge nicht nur längere Inaktivität festzustellen sondern auch die Richtigkeit der Daten zu hinterfragen. Die gesetzliche Anordnung ist nicht dahingehend zu interpretieren, dass sie einen Rechtfertigungsgrund für eine dauerhafte Speicherung bzw. Verarbeitungs sämtlicher Daten darstellt, die dem Diensteanbieter im Wege der Registrierung bekannt werden.

Entsprechend Art. 17 DSGVO ist das Recht des Nutzers vorgesehen, zu verlangen, dass sein Registrierungsprofil unverzüglich gelöscht wird. Zudem hat der Diensteanbieter ein Registrierungsprofil nach einer längeren Periode der Inaktivität, wobei im Sinne der Rechtsklarheit hier der Zeitraum von einem Jahr festgelegt wird, zu löschen. Diese Anordnung bedeutet nicht, dass der Diensteanbieter zu prüfen hätte, ob der Poster regelmäßig Postings veranlasst, sondern es geht um die Frage, ob der registrierte Nutzer überhaupt das Online-Informationsangebot länger schon nicht genutzt hat.

Es ist weiters davon auszugehen, dass die Diensteanbieter ihrerseits den Vorgaben der DSGVO oder vergleichbarer Normen unterliegen.

Zu § 4:

In den verschiedenen Absätzen des § 4 wird deutlich gemacht, in welchen Fällen der Diensteanbieter die aufgrund der Verpflichtungen nach diesem Bundesgesetz „gesammelten“ personenbezogene Daten an Dritte weitergeben darf. Die in diesem Gesetz verwendeten Begrifflichkeiten sind im Sinne der DSGVO zu verstehen. So handelt es sich bei der „Verarbeitung“ (vgl. Art. 4 Z 2 DSGVO) um *„jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;“*.

Abs. 1 und 2 stellen im Vergleich zur bislang geltenden Rechtslage den grundsätzlichen „Mehrwert“ des Entwurfs dar, zumal § 90 Abs. 7 TKG und die Parallelnorm in § 76a Abs. 1 StPO gerade keine Möglichkeit für Dritte vorsehen, im Falle von Straftaten in Form der Privatanklagedelikte in § 111 und 115 StGB oder in den Fällen der Verfolgung zivilrechtlicher Ansprüchen wegen *„Verletzungen an der Ehre“* die Identität des Nutzers durch Zugang zu den Stammdaten des Betreibers des Telefondienstes herauszufinden. Dieses Defizit soll durch den Entwurf beseitigt, gleichzeitig aber dafür Sorge getragen werden, dass der Diensteanbieter nur in sachlich begründeten Fällen die betreffenden Daten herausgibt, die es ermöglichen, vom Betreiber des Telefondienstes die von ihm verarbeiteten Stammdaten des betreffenden Posters zu verlangen. Die dritte Person hat daher glaubhaft zu machen, dass ihr kein anderer Weg zur Verfügung steht, um für die Erhebung der Privatanklage oder die Verfolgung allfälliger Ansprüche nach § 1330 ABGB zur wahren Identität des Posters zu gelangen. Gesondert ist erneut darauf hinzuweisen, dass – wie § 4 Abs. 4 des Entwurfs dies eindeutig regelt – beim Diensteanbieter keinerlei Verknüpfung zwischen der Identität eines Posters und dem Inhalt eines Postings vorgenommen werden darf.

Es liegt in dieser Hinsicht nahe, gerade auch im Bereich der gerichtlichen Straftaten in Form von Officialdelikten den betreffenden Gerichten und Staatsanwaltschaften die Daten zur Verfolgung zur Verfügung zu stellen, um diese etwa in Fällen der Verhetzung beim Zugang zu bestimmten Daten des Straftäters nicht schlechter zu stellen als den in seinen Persönlichkeitsrechten verletzten Dritten.

Selbstverständlich gilt die Auskunftsverpflichtung gegenüber Dritten nur für den durch ein Posting in seinem Recht auf Schutz der Ehre beeinträchtigten Dritten. Gesondert ist erneut darauf hinzuweisen, dass – wie § 4 Abs. 4 des Entwurfs dies eindeutig regelt – beim Diensteanbieter keinerlei Verknüpfung zwischen der Identität eines Posters und dem Inhalt eines Postings vorgenommen werden darf.

Zu § 5:

Zur Effektuierung der von diesem Bundesgesetz dem Diensteanbieter auferlegten Pflichten wird nach dem Vorbild des verantwortlichen Beauftragten in § 9 VStG – allerdings zwingend und nicht nur fakultativ oder im Einzelfall im Auftrag einer Behörde – vorgesehen, dass ein verantwortlicher Beauftragter zu bestellen ist. Der Beauftragte sollte unverzüglich erreicht werden können, worunter im Regelfall eine Erreichbarkeit binnen spätestens 12 Stunden zu verstehen sein wird. Dies gilt aufgrund des Wesens der hier geregelten Sachmaterie unabhängig von der Frage, ob es sich bei dem Zeitpunkt, in dem versucht wird, den Beauftragten zu erreichen, um einen Werktag handelt oder nicht.

Zu §§ 6 bis 8:

Die Regelungen nehmen die Aufgabenzuweisung vor (§ 6) und enthalten den Sanktionskatalog bestehend aus Geldbußen und Geldstrafen (§§ 7 und 8).

Im Hinblick auf die Frage der „Schwere des Vergehens“ sind auch bei der Verhängung von Geldbußen zumindest dem Grundsatz nach general- und spezialpräventiven Überlegungen, jedenfalls aber Sachlichkeitsüberlegungen im Sinne der „Vorwerfbarkeit“, Zumutbarkeit und der Angemessenheit anzustellen. Deswegen sieht § 7 Abs. 2 einen Katalog zu berücksichtigender Aspekte vor. Beim Ausmaß und der Dauer der Nachlässigkeit der Einhaltung der Bestimmung wird etwa das Vorhandensein eines Kontrollsystems und die Maßnahmen zur Überwachung dieses Kontrollsystems zu berücksichtigen sein. Beim Grad der „Intentionalität“ geht es um die Prüfung, ob ein „systematisches Ignorieren“ oder allenfalls auch ein komplexer hoher Organisationsgrad zur Duldung/Begünstigung gesetzwidrigen Verhaltens, geführt hat oder tatsächlich eine „entschuldbare Fehlleistung“ vorliegt. Das Verfahren zur Verhängung einer Geldbuße ist nicht als Strafverfahren zu qualifizieren (vgl. zum Nebeneinander von Geldbuße und Geldstrafe VfGH 13.12.2016 E 729/2016-18).

Zur Frage, ob auch wiederholt eine Strafsanktion verhängt werden kann, wenn ein Anbieter trotz einer (auf einen bestimmten Zeitraum bezogenen) Feststellung über einen Verstoß gegen Handlungspflichten weiterhin nichts unternimmt, um die vom Gesetz geforderte Handlung zu setzen (etwas die Bestellung eines verantwortlichen Beauftragten), ist Folgendes festzuhalten: Feststellungen über Rechtsverletzungen erfolgen immer im Hinblick auf einen konkreten Zeitraum. Ein Dauerdelikt (dh das dauernde Unterlassen) endet spätestens mit seiner Bestrafung, sodass späteres strafbares Verhalten neuerlich verfolgt werden kann (vgl. zum Dauerdelikt *Hengstschläger/Leeb*, *Verwaltungsverfahrensrecht*⁵, Rz 771, S 421).

Zur Höhe der Geldbußen und zur Zulässigkeit der Verhängung hoher Geldbußen durch eine Verwaltungsbehörde ist auf das Erkenntnis des VfGH vom 13. Dezember 2017, G 408/2016, zu verweisen (Pressemeldung abrufbar unter https://www.vfgh.gv.at/downloads/VfGH_Presseinfo_G_408-2016_ua_Bankwesengesetz.pdf).

Zu § 9:

Entsprechend dem *best effort*-Grundsatz normiert diese Regelung, dass eine Verantwortlichkeit ausscheidet, wenn sich der Diensteanbieter bzw. der verantwortliche Beauftragte mit der gebotenen Sorgfalt, dh. nach bestem Wissen und Gewissen, darum bemüht hat, den gesetzlichen Anforderungen zu entsprechen, dennoch aber das angestrebte Ziel der Identifikation des Nutzers nicht erfüllt werden konnte.

Zu Art. 2 (Änderung des KommAustria-Gesetzes)**Zu Z 1 (§ 2 Abs. 1 Z 13), Z 2 (§ 13 Abs. 4 Z 4) und Z 3 (§ 17 Abs. 1 Z 5):**

Die Änderungen ergeben sich aus den nach dem SVN-G begründeten neuen Aufgaben für KommAustria und RTR-GmbH.

Zu Z 4 (§ 35a):

Im Hinblick auf die bisherige – durch die Judikatur des VfGH (vgl. VfSlg. 17326/2004) vorgezeichnete – Systematik, wonach die Finanzierung der Tätigkeit der KommAustria und der RTR-GmbH (und auch der TKK etc.) aus einem Beitrag der „Allgemeinheit“ und Finanzierungsbeiträgen der unterschiedlichen Branchen (vgl. §§ 34 bis 35) erfolgt, ist für den hinzutretenden Aufwand der Aufsicht über die betreffenden Dienste der Informationsgesellschaft eine eigene Beitragsregelung vorzusehen. Dabei wird davon ausgegangen, dass 100 % der darauf bezogenen Tätigkeit der beiden Institutionen aus den Mitteln des Budgets zu finanzieren sein werden. Im Übrigen ist in § 10 Abs. 3 vorgesehen, dass 50 % des Betragseiner Geldbuße für die Zwecke der Vollziehung der Anordnungen dieses Bundesgesetzes der KommAustria (und der RTR-GmbH) zuzuweisen sind.

11. Abstract (Deutsch)

In den letzten Jahren hat sich bei der Kommunikation im Internet die stetig steigende Zahl von untergriffigen und mitunter rechtswidrigen Kommentaren zu einem zunehmenden Problem entwickelt. Als mögliches Mittel, um dem „Hass im Netz“ entgegenzuwirken, wird oftmals die Einführung einer Identifizierungspflicht ins Spiel gebracht. Im Sinne einer „digitalen Ausweispflicht“ sollen dabei sämtliche Nutzer von Diskussionsplattformen dazu verpflichtet werden, vorab ihre Identitätsdaten beim Plattformbetreiber zu hinterlegen. Bei der Variante einer Klarnamenpflicht wäre darüber hinaus auch die Verwendung von Pseudonymen bzw Nicknames nicht mehr erlaubt. Auf diese Weise soll die Anonymität in Foren beseitigt und die Identität der Verfasser von Hasspostings jederzeit festgestellt werden können. Befürworter der Anonymität hingegen sehen durch einen solchen Identifizierungszwang die Ausübung der freien Meinungsäußerung im Netz gefährdet.

Im Jahr 2019 hat die damalige österreichische Bundesregierung mit dem Ministerialentwurf für ein „Bundesgesetz über Sorgfalt und Verantwortung im Netz“ (SVN-G) erstmals den Entwurf eines vollständigen Gesetzes vorgelegt, das eine solche Identifizierungspflicht vorsieht. Auch wenn dieser Entwurf in der Folge nicht umgesetzt und auch von den Nachfolgeregierungen bis dato nicht mehr weiterverfolgt worden ist, bedeutet dies keinesfalls, dass die Einführung einer Klarnamen- bzw Identifizierungspflicht zukünftig ausgeschlossen ist, da die Forderungen nach gesetzlichen Maßnahmen gegen Hasspostings nicht verstummt sind.

Das Ziel dieser Arbeit ist es daher, anhand einer umfangreichen Analyse und anschließender Grundrechtsprüfung am Beispiel des Ministerialentwurfs des SVN-G zu beurteilen, ob eine Identifizierungs- bzw Klarnamenpflicht ein geeignetes Mittel darstellt, um dem Problem „Hass im Netz“ effektiv entgegenzuwirken und ob die Umsetzung einer solchen Maßnahme in Österreich möglich wäre, ohne dabei die Grundrechte der Bürger, welche die betroffenen Diskussionsforen nutzen, zu verletzen.

12. Abstract (English)

In recent years the steadily increasing number of malicious comments adversely affected the communication on the Internet. As a possible measure of counteracting hate speech the introduction of a mandatory identification for users of Internet forums is often suggested. Such a measure would require all users of affected online platforms to disclose their identities including their real names in advance to the platform operator in a mandatory registration process before commenting. With the variant of a so-called real-name system the use of pseudonyms or nicknames would also no longer be permitted. This would eliminate anonymity from Internet forums and as a result the identity of any user could easily be investigated. On the other hand, advocates for anonymity are voicing concerns that such mandatory identification would seriously jeopardize the exercise of freedom of expression on the Internet.

In 2019 the then Austrian federal government for the first time presented the draft law for such a mandatory identification, the so-called "Federal Act on Diligence and Responsibility on the Web". Despite the fact that this draft was not subsequently pursued or implemented to this day, this does not mean that the introduction of an identification requirement or a real-name system can be ruled out in the future, as the discussions about legal measures against hate speech are still going on.

Therefore, the aim of this thesis is, by assessing the draft of the "Federal Act on Diligence and Responsibility on the Web", to conduct an in-depth scrutiny for its conformity with fundamental rights, to evaluate whether a mandatory identification or a real-name system would be a viable measure to effectively counteract hate speech and whether the implementation of such a measure would be feasible in Austria without violating the fundamental rights of the citizens who use the affected online platforms.